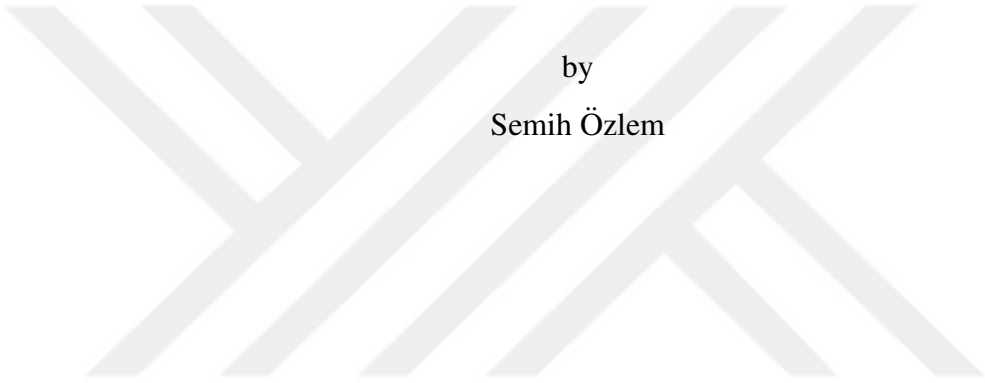


ON THE MOTIVIC GALOIS GROUP OF A NUMBER FIELD

by
Semih Özlem



Submitted to Graduate School of Natural and Applied Sciences
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy in
Mathematics Department

Yeditepe University

2021

ON THE MOTIVIC GALOIS GROUP OF A NUMBER FIELD

APPROVED BY:

Prof. Dr. Ender Abadoğlu

.....

(Thesis Supervisor)

(Yeditepe University)

Prof. Dr. Kâzım İlhan İkedâ

.....

(Thesis Co-Supervisor)

(Boğaziçi University)

Prof. Dr. Sinan Ünver

.....

(Koç University)

Dr. Öğr. Üyesi Erol Serbest

.....

(Yeditepe University)

Dr. Öğr. Üyesi Sevan Bedikyan

.....

(Mimar Sinan Güzel Sanatlar Üniversitesi)

Dr. Öğr. Üyesi Mehmet Akif Erdal

.....

(Yeditepe University)

DATE OF APPROVAL: /.... /2021

I hereby declare that this thesis is my own work and that all information in this thesis has been obtained and presented in accordance with academic rules and ethical conduct. I have fully cited and referenced all material and results as required by these rules and conduct, and this thesis study does not contain any plagiarism. If any material used in the thesis requires copyright, the necessary permissions have been obtained. No material from this thesis has been used for the award of another degree.

I accept all kinds of legal liability that may arise in case contrary to these situations.

Name, Last name

Signature



ACKNOWLEDGEMENTS

I am in gratitude to my thesis advisor Kâzım İlhan İkedâ for his continual encouraging attitude and for guiding me to look at things that bring out amazement and surprise, for suggesting topic of this thesis, and introducing me to Langlands program and number theory. I am also thankful to Yeditepe University and my thesis co-advisor Ender Abadoğlu for raising interesting questions to ponder upon.

I thank my thesis committee for taking time to read this thesis. I also thank Yeditepe Mathematics Department and my family for supporting me during the writing of this thesis.

I thank the authors of all the sources that I have used, whose dedication and commitment to writing their ideas inspired and challenged me into writing this thesis.

I also thank everyone who has helped or influenced me directly or indirectly to get seriously involved in mathematics and come to this day to write this thesis, including my math teachers and professors and friends. I thank developers of Linux, Ubuntu, Debian, and Knoppix and people in Linux, Ubuntu, Debian and Knoppix users group, whose answers helped in maintaining a Linux computer system functional and running to write this thesis.

I thank Bursa İl Halk Kütüphanesi for providing space to study in earlier part of this thesis.

Last but not least, I thank my family, my father, mother and brother. Without their emotional and material support this thesis would not come to fruition.

ABSTRACT

ON THE MOTIVIC GALOIS GROUP OF A NUMBER FIELD

In this thesis, it is proved that there is a homomorphism from Weil-Arthur idèle group to Taniyama group, which is isomorphic to the motivic Galois group of CM motives. Furthermore if James Arthur's construction of Langlands' group is valid, and the group $\mathcal{G}_F$ that he constructs is indeed isomorphic to the motivic Galois group then there is a commutative diagram that these groups fit inside.

In order to lay the foundations for these groups, there is a review of (i) category theory, (ii) algebraic geometry, (iii) Tannakian categories, (iv) motives and motivic Galois group, (v) Alexander Grothendieck's standard conjectures, (vi) Weil group and Artin Reciprocity of number theory, (vii) construction of Serre-Taniyama group, (viii) James Arthur's construction of Langlands' group, (ix) Complex Multiplication, Abelian Varieties, and CM motives.

ÖZET

BİR SAYI CİSMİNİN MOTİFSEL GALOİS GRUBU ÜZERİNE

Bu tezde Weil-Arthur idèle grubundan Taniyama grubuna bir homomorfizma var olduğu ispat edilmiştir. Taniyama grubu, CM motiflerinin motifsel Galois grubuna izomorftur.

Ayrıca, James Arthur'un Langlands grubunun inşası doğru olduğu ve inşasını belirttiği $\mathcal{G}_F$ grubu motifsel Galois grubuna izomorf olduğu takdirde, bu grupların yer aldığı bir komütatif (değişmeli) diyagram vardır.

Bu grupların tanımları için gerekli olan temel kavramlar ünitelerde açıklanmıştır. Bu konular: (i) kategori teorisi, (ii) cebirsel geometri, (ii) Tannaka kategorileri, (iii) motifler ve motifsel Galois grubu (iv) Alexander Grothendieck'in standart varsayıları (v) Weil grubu ve Artin Eşlenikselliği (vi) Serre-Taniyama grubunun inşası, (vii) James Arthur'a ait olan Langlands Grubunun inşası (vii) Kompleks Çarpım (CM - KÇ), Abelyen Varyeteler, KÇ - Motifleri (CM-Motifleri) dir.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	iv
ABSTRACT	v
ÖZET	vi
1. INTRODUCTION	1
2. CATEGORY THEORY BACKGROUND	3
2.1. CATEGORY THEORY BASICS	3
2.1.1. Categories.....	3
2.1.2. Subobject	16
2.1.3. Functors, Natural Transformations	20
2.1.4. Product, Coproduct (Sum) of a Family of Objects.....	24
2.1.5. Product of Categories	27
2.1.6. Multifunctors	28
2.1.7. Godement Product, Categories of Functors.....	28
2.1.8. Equivalence of Categories	31
2.1.9. More Category Theory Basics: Faithful, Fully Faithful Functor etc.....	32
2.1.10. Representable Functor, Yoneda Lemma	36
2.1.11. Group of Automorphisms of a Functor, and its Action.	37
2.2. AB-CATEGORY, PREADDITIVE CATEGORY, ABELIAN CATEGORY	38
2.2.1. Preadditive Categories, A -linear Categories	38
2.2.2. Kernel, Cokernel, Zero (Null) Object, Image, Coimage, Pullback, Pushout/Pushforward, Product, Sum, Biproduct	39
2.2.3. Abelian Category	44
2.2.4. Pseudo-abelian Categories	45
2.3. RADICAL OF A CATEGORY	47
2.4. SEMISIMPLE CATEGORIES.....	48
2.5. LIMIT, COLIMIT, PROJECTIVE AND INJECTIVE LIMIT.....	50
2.5.1. Colimit and Limit	50
2.5.2. Projective and Injective Limits	51
2.5.3. Compatibility of Category-theoretic Definition and Algebraic Definition ..	54
2.5.4. When Direct and Inverse Limits are Nonempty	60

2.5.5. Morphism between two Direct and Projective Limits	61
3. ALGEBRAIC GEOMETRY	62
3.1. SCHEMES.....	62
3.1.1. Spec of a Ring, Zariski Topology	62
3.1.2. Remark on Products	63
3.1.3. Elements of the Ring as Functions on Spec of the Ring	64
3.1.4. Polynomials over an Algebraically Closed Field.....	64
3.1.5. Sheaves	65
3.1.6. Sheaf on Spec of a Ring	70
3.1.7. Scheme	71
3.1.7.1. Preliminary Definitions for a Scheme.....	71
3.1.7.2. Definition of an Affine Scheme and Scheme.....	73
3.1.8. Smoothness.....	74
3.1.9. Projective Schemes	75
3.2. PROPERTIES OF SCHEMES	76
3.2.1. Properties of Morphisms of Schemes: Locally of Finite Type, of Finite Type, Finite Morphism.....	77
3.2.2. Algebraic Scheme, Closed Subscheme.....	78
3.3. PRODUCT OF SCHEMES	78
3.4. VARIETY	79
3.4.1. Closed Subschemes	81
3.4.2. Sheaf of Modules, Quasi-coherent Sheaf.....	82
3.4.3. Projective Variety	83
3.4.4. Separated Morphism.....	83
3.4.5. Proper Morphism, Complete Variety, Generic Point	83
3.5. GROUP SCHEME, GROUP VARIETY, HOMOGENEOUS SPACE	84
3.5.1. Affine Group Scheme	85
4. TANNAKIAN CATEGORIES	86
4.1. TENSOR CATEGORIES ($\otimes$ -CATEGORIES)	86
4.2. ASSOCIATIVITY CONSTRAINTS.....	90
4.3. COMMUTATIVITY CONSTRAINTS.....	92
4.4. UNIT CONSTRAINTS	93

4.5. COMPATIBILITY AMONG CONSTRAINTS.....	101
4.5.1. Associativity and Commutativity	101
4.5.1.1. Remark on Associativity and Commutativity Constraint.....	102
4.5.2. Associativity and Unit.....	109
4.5.3. Commutativity and Unit.....	111
4.5.4. Associativity, Commutativity and Unit.....	112
4.6. INVERTIBLE OBJECTS	112
4.7. TANNAKIAN CATEGORIES.....	113
4.7.1. Internal Hom.....	113
4.7.2. Tensor Functors	116
4.7.3. Tensor Equivalences	119
4.7.4. Rigid Tensor Category	120
4.7.5. Neutral Tannakian Category.....	120
4.8. REPRESENTATIONS	121
5. MOTIVES AND MOTIVIC GALOIS GROUP	122
5.1. INTRODUCTION.....	122
5.2. INTERSECTION THEORY AND OTHER PRELIMINARIES.....	122
5.3. ADEQUATE EQUIVALENCE RELATION.....	125
5.4. WEIL COHOMOLOGY	127
5.5. MOTIVES	129
5.6. MOTIVIC GALOIS GROUP	130
5.6.1. What is known or assumed about the Motivic Galois Group	130
5.6.2. Motivic Galois Group and Galois Group	131
6. STANDARD CONJECTURES.....	132
6.1. STATEMENT OF STANDARD CONJECTURES	132
6.1.1. Grothendieck's Formulation.....	132
6.1.2. Other formulations of the Conjectures by Grothendieck.....	132
6.1.3. Steven Kleiman's Restatement	135
6.2. RATIONALE	135
6.2.1. Summary of Serre's Article.....	136
6.2.2. Weil Conjectures.....	138
7. WEIL GROUP AND ALGEBRAIC NUMBER THEORY	139

7.1. PRELIMINARIES.....	139
7.1.1. Weil Group's Definition in Tate's Number Theoretic Background (NTB) ..	139
7.1.2. Construction of Weil group, Tate - NTB	141
7.1.3. Consequences of the Canonical Class Isomorphism	145
7.1.4. Uniqueness of Weil Group	148
7.1.5. Special Cases	149
7.1.6. Automorphisms of Weil Group	151
7.1.7. Local-Global Relationship	151
7.2. ARTIN RECIPROCITY	152
7.2.1. Reciprocity Law isomorphism and Norm-Residue Map	155
7.2.2. Abelian Extensions and Norm Groups	158
7.2.3. Weil Group as in Shih	158
7.3. NOTATION.....	162
7.4. RELATIVE WEIL GROUP AND WEIL GROUP QUOTIENTS	162
7.5. ATTEMPTS TO COMBINE THE DIAGRAMS OF PREVIOUS SECTION WITH WEIL GROUP DIAGRAMS	172
7.6. SOME EXACT SEQUENCES	173
7.7. LEMMAS FOR NUMBER THEORETIC BACKGROUND	176
7.8. TRANSFER MAP	180
7.9. SEMIDIRECT PRODUCTS	189
8. SERRE-TANIYAMA GROUP	200
8.1. NOTATION, BACKGROUND	200
8.2. KRULL TOPOLOGY ON GALOIS GROUPS OF INFINITE EXTENSIONS.	200
8.3. ENLARGING GROUP	201
8.4. IDELÈS and Idelès-classes	215
8.4.1. Topology of Idele Group.	216
8.4.2. Embedding of K^* inside Ideles and Idele Class Group	216
8.4.3. Modulus of Support and Exact Sequence	216
8.5. RESTRICTION OF SCALARS	220
8.6. THE TORUS T	221
8.6.1. Subgroups of Tori	222
8.7. ALGEBRAIC TORI	223

8.7.1. Splitting Fields	229
8.8. CHARACTERS OF MULTIPLICATIVE GROUP	229
8.9. CONSTRUCTION OF SERRE-TANIYAMA GROUP	231
8.10. GROUP COHOMOLOGY RESULTS	234
8.10.1. Different Sections	236
8.10.2. Further Lemmas	242
8.10.3. Further Discussion	271
8.11. EXACT SEQUENCES WITH RELATIVE WEIL GROUPS, LOCAL AND GLOBAL	283
8.12. LANGLANDS' CONSTRUCTION OF TANIYAMA GROUP, MAP FROM WEIL GROUP TO TANIYAMA GROUP	284
9. ARTHUR'S CONSTRUCTION OF LANGLANDS GROUP.....	297
9.1. SUMMARY	297
9.2. PRELIMINARIES.....	299
9.2.1. Tits System	299
9.2.2. Reductive Group, Quasisplit	299
9.2.3. Theorem on Reductive Groups and Root Systems	300
9.2.4. Automorphic Representation.....	300
9.2.5. L -group and L -homomorphism	300
9.2.6. Automorphic Family and $\mathcal{C}_{\text{aut}(G)}$	301
9.2.7. Type A_0	301
9.2.8. Weil-Taniyama Group	301
10. COMPLEX MULTIPLICATION, ABELIAN VARIETIES AND PLECTIC	303
10.1. COMPLEX MULTIPLICATION	303
10.2. HODGE CYCLES AND MOTIVES.....	304
10.2.1. Hodge Cycles on Abelian Varieties	304
10.2.2. Tannakian Categories.....	305
10.2.3. Langlands' Construction of Taniyama Group	306
10.2.4. Motives and Taniyama Group.....	307
10.3. ABELIAN VARIETIES	307
10.4. ABELIAN VARIETIES AND COMPLEX MULTIPLICATION	309

10.4.1. l -adic Representations of Homomorphisms	309
10.4.2. Riemann Form.....	310
10.4.3. Polarization of a Variety	310
10.4.4. Picard Variety.....	311
10.4.5. Analytic Coordinate System of an Abelian Variety.....	313
10.4.6. Rational and Analytic Representations.....	313
10.4.7. CM-types	314
10.5. DELIGNE'S RESULT ON CM MOTIVES AND TANIYAMA GROUP	315
10.5.1. Motives	315
10.5.2. Artin Motives	316
10.5.3. CM Motives.....	316
10.6. PLECTIC TANIYAMA GROUP.....	317
11. MAIN RESULTS.....	319
11.1. GENERAL IDEAS.....	319
11.2. MAIN RESULTS – SKETCH	321
11.3. AUTOMORPHISM GROUP OF A FUNCTOR.....	324
12. CONCLUSIONS	327
REFERENCES	331

1. INTRODUCTION

Samuel Eilenberg and Saunders Mac Lane introduced basic concepts of category theory for aiding study of algebraic topology [27]. These concepts were also applicable in algebraic geometry. Category theory provides a useful language and setting for algebraic geometry and algebraic topology by translating problems of a geometric or topological nature to algebraic problems. Instead of formulating common problems in different settings with different tools, category theory provides a mechanism of gathering those common tools in one language.

The abstraction of a scheme comes out of considering the function field on a variety, and how the algebraic properties of the function field relate to geometric or topological properties of the variety. Scheme theory also provides a useful language to consider how points on a variety change as one changes the number field that the variety is defined in.

In 1969 Alexandre Grothendieck formulated Standard Conjectures in algebraic geometry. These conjectures came out of observations or partial results in algebraic geometry that involved cohomology, intersection theory, and Weil's conjectures. He also introduced Motivic Galois Group, generalizing the Galois group of field theory to varieties.

By Künneth formulas, product of varieties gets translated to tensor product in cohomology. Because of this and many other reasons, tensor categories, and Tannakian formalism proved to be useful in the construction and hopefully proving properties of Motivic Galois group, at least by assuming some of the standard conjectures.

Serre gave a construction of Serre-Taniyama group, which was also carried out in papers by Deligne-Milne, and Langlands. The significance of Serre-Taniyama group is tied to l -adic representations, however this is not really discussed in this work. Serre's book [84] is a good source for those who want to get into this.

It was proved by Deligne that the Taniyama group is isomorphic to the motivic Galois group of CM motives.

Results by Yves Andre, Uwe Jannsen, determined further properties of Motivic Galois group. In particular, reliance on standard conjectures could partially be lifted.

Construction of Serre-Taniyama group, and arguments given in the map from Weil group to Taniyama group rely on second group cohomology which classifies group extensions.

Langlands postulated and James Arthur gave a potential construction for Langlands' group. This group came out of consideration of automorphic representations, and potential deep links in number theory, that start with Weil group and Artin reciprocity, and possible generalizations of reciprocity, through considerations of Abelian varieties.

Lately, using nonabelian reciprocity, K. I. Ikeda described morphisms from Weil-Arthur idèle group to Langlands' group, assuming James Arthur's construction.

In this thesis I review these results, and prove that there is a morphism from Weil-Arthur idèle group to Taniyama group, through the established morphisms, and prove that if we assume Arthur's construction, Weil-Arthur idèle group, Langlands' group, and Taniyama group, and nonabelian idèle group fit into a commutative diagram. The significance of this result is to place the elusive groups of Langlands and motivic Galois group in a diagram of groups whose properties may be better known or captured.

2. CATEGORY THEORY BACKGROUND

2.1. CATEGORY THEORY BASICS

2.1.1. Categories

There are many sources on category theory. The following sources have been closely followed: [33], [65], [68], [1]. The definitions follow [33] more closely, and they are supplemented with variations in the remaining other sources. There are some new definitions that build upon the existing definitions. For example the notion of factoring through is used in the literature without being defined explicitly. The example given for subobjects with unit circle S^1 as subobject under different embeddings into torus $S^1 \times S^1$ does not come from a source, though it may appear in sources I am not aware of, maybe in algebraic topology texts.

The notion of a category is a generalization of almost any mathematical structure or theory. The most basic category is formed from the notion of sets (as objects) and functions between sets (as morphisms). Another example of a category comes from linear algebra, with vector spaces over a fixed field (objects) and linear transformations from one vector space into another (as morphisms). What is common in these (and many other) cases is abstracted to give the notion of a category.

First there is a collection called *the collection of objects*. In case of set theory this collection would be a collection of sets, in case of vector spaces it would be vector spaces over a fixed field. There is really no restriction on this collection (other than that it be nonempty).

Associated to each pair of objects, there is a set called *morphisms* from the first object into the second. In the example of sets this would be the set of all functions from one set into another. In the case of vector spaces it would be the set of all linear transformations from one vector space into another. The first object in the pair is referred as *domain* or *source* or *departure of the morphism*, the second object in the pair is referred as *codomain* or *target* or *arrival of the morphism*. The morphism is said to be a morphism from its source object to its target object. This is written in the notation $f : A \rightarrow B$, as in ordinary set theory, to denote that f is a morphism from object A into object B . The set of morphisms from object A into object B in what is called category $\mathbf{C}$ will be denoted by $\text{Hom}_{\mathbf{C}}(A, B)$.

Associated to each pair of morphisms, when the target of the first morphism and the source of the second morphism is identical, there is an operation called *composition of morphisms* that associates a morphism from the source of the first morphism in the pair to the target of the second morphism in the pair. This is formally written in the following fashion: when $f : A \rightarrow B$ and $g : B \rightarrow C$, then target of f and source of g are the same object B , hence they can be composed to give $\text{composition}(f, g) = g \circ f : A \rightarrow C$ a morphism from the source object A of the first morphism in the pair, i.e. f , into the target object C of the second morphism in the pair, i.e. g . Formally this is written by stating that for each triple of objects A, B, C of the category $\mathbf{C}$ there is a function

$$\text{composition}_{A,B,C} = c_{A,B,C} = c : \text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(B, C) \rightarrow \text{Hom}_{\mathbf{C}}(A, C) \quad (2.1)$$

This function should be *associative* in the following sense. Using such a composition function, when we consider a quadruple, or 4–tuple, of objects (A, B, C, D) in a category $\mathbf{C}$, there are two different ways of defining a composition in that order. If we shorten composition to c , and denote by $c(f, g) = g \circ f$ the composition of f and g when target f and source g are the same, then $c(c(f, g), h)$ and $c(f, c(g, h))$ are two different compositions. Associativity is requiring that these two different compositions be identical.

Explicitly given

$$c_{X,Y,Z} : \text{Hom}_{\mathbf{C}}(X, Y) \times \text{Hom}_{\mathbf{C}}(Y, Z) \rightarrow \text{Hom}_{\mathbf{C}}(X, Z) \quad (2.2)$$

for any three objects X, Y, Z in the category $\mathbf{C}$, we define left-initiated 4–tuple composition

$$cl_{A,B,C,D} : \text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(B, C) \times \text{Hom}_{\mathbf{C}}(C, D) \rightarrow \text{Hom}_{\mathbf{C}}(A, D) \quad (2.3)$$

and right-initiated 4–tuple composition

$$cr_{A,B,C,D} : \text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(B, C) \times \text{Hom}_{\mathbf{C}}(C, D) \rightarrow \text{Hom}_{\mathbf{C}}(A, D) \quad (2.4)$$

by

$$cl_{A,B,C,D}(f, g, h) = c(c(f, g), h) = h \circ (g \circ f) \quad (2.5)$$

and

$$cr_{A,B,C,D}(f, g, h) = c(f, c(g, h)) = (h \circ g) \circ f \quad (2.6)$$

Associativity is the condition

$$cl_{A,B,C,D} = cr_{A,B,C,D} \quad (2.7)$$

for any four objects A, B, C, D in the category $\mathbf{C}$.

Of course this is assuming that when we take a triplet or a quadruplet, this is uniformly defined so that there really is not a circularity of definition here. In other words one assumes set theory and proceeds to construct category theory on top. I am not aware of a way of defining category theory without set theory as the definition itself assumes it. Or one needs to assume something like set theory to speak of collections, finite products of sets whose elements are ordered pairs, ordered triplets, ordered quadruplets, ordered n -tuples etc. It is assumed that whatever a collection is, it already has the notion of ordered pair from the collection, ordered triplet, ordered quadruplet. This notion certainly exists if the collection itself is a set. Otherwise it is simply assumed that, say, there is such a thing as the collection (class) of all “functions” from finite sets into the collection (class) of objects of the category.

Composition of functions in set theory, or composition of linear transformations from one vector space into another are associative, almost directly by definition of composition.

In category theory objects themselves do not have to be sets, and hence we do not work with elements of an object, although in set theory or most of mathematics we work with elements of a set when working with functions among them. In any mathematical theory founded on sets and functions, possibly with additional structures imposed on the set and functions, a function from one set to another, defines a function from the power set of the domain into the power set of the codomain called the image, and a function from the power set of the codomain into the power set of the domain called preimage. These are not a priori defined on categories, but must be built up by using the notion of subobjects. The notion of a subset does not immediately extend into category theory.

The other requirement of the definition of category involves existence of a morphism called *identity morphism* associated to each object of the category, from and into that object (such

things are called *endomorphisms* of an object), such that when composed with any morphism with which it is composable, this gives the same morphism. Formally this is written as follows: There is a morphism $1_B \in \text{Hom}_{\mathbf{C}}(B, B)$ for every object B such that for all objects A and C in $\mathbf{C}$, and all morphisms $f \in \text{Hom}_{\mathbf{C}}(A, B)$ and $g \in \text{Hom}_{\mathbf{C}}(B, C)$, $c(f, 1_B) = 1_B \circ f = f$ and $c(1_B, g) = g \circ 1_B = g$.

This is summarized in the statement:

Definition 1 A *category* consists of

- (i) a collection of **objects** and
- (ii) corresponding to each pair of objects in the collection a set called **morphisms** from the first object of the pair into the second object in the pair, such that the morphism sets are disjoint for distinct pairs
- (iii) for any three objects A, B, C , a function called **composition** from the product of the set of morphisms from A into B , and the set of morphisms from B into C , into the set of morphisms from A into C such that
 - (iii.i) composition is **associative** in the sense above whenever defined
 - (iii.ii) corresponding to each object there is a morphism from that object into itself called **identity** which acts as both left and right identity of composition.

The reason for calling the collection of objects a collection as opposed to a set is to avoid problems related to Russell's paradox. There is no such thing as the set of all sets, since assuming existence of the set of all sets S , and assuming one can define subset of any set satisfying a property P , which is a formula of one variable, would imply that one can write a set $S' = \{x \in S \mid x \notin x\}$, i.e. a set which contains (has as elements) those sets that are not elements of themselves. But then $S' \in S'$ if and only if $S' \notin S'$, which is a contradiction. Alternatively assuming that formation of the power set of a set strictly increases cardinality, one obtains a contradiction. In order to circumvent this paradox, one calls the entity which would contain any set as a class or collection, something that is not in the same logical type as a set, but something higher. However it is not the main aim of this thesis to go into logical foundations, so I will not go further into defining what a collection or class means. One can look up classes in [77, Part 1, Chapter VI, pages 66-81], or other books on axiomatic

foundations of set theory, or the theory of universes by Grothendieck and others in SGA4, specifically beginning of the chapter on presheaves [38] and the appendix to that chapter [13], or [70, pages 37-38].

From now on we will simply assume that there exists a category on a collection of sets, whose objects are elements of the collection of sets in consideration, whose morphisms are all functions from one set in the collection into another set in the collection.

In a category, when the collection of objects is a set, the category is called *small*. Also it is not correct to view the assignment that assigns to each pair of objects its corresponding morphism set a function. However when the category is small, this can be viewed as such, since one can then speak of the set whose elements are morphism sets. In other words if $\text{Ob}(\mathbf{C})$ denotes the set of all objects of a small category, then

$$\text{Hom}_{\mathbf{C}} = \{\text{Hom}_{\mathbf{C}}(A, B) \mid (A, B) \in \text{Ob}(\mathbf{C})^2\} \quad (2.8)$$

is a set, and the function

$$\text{Ob}(\mathbf{C})^2 \rightarrow \text{Hom}_{\mathbf{C}}$$

defined by

$$(A, B) \mapsto \text{Hom}_{\mathbf{C}}(A, B)$$

is a function. In such a case composition is defined on $\sqcup_{A,B,C \in \text{Ob}(\mathbf{C})} \text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(B, C)$ and into $\sqcup_{A,C \in \text{Ob}(\mathbf{C})} \text{Hom}_{\mathbf{C}}(A, C)$, such that the set product corresponding to any triplet (A, B, C) of objects is mapped into the set corresponding to the pair (A, C) of objects. In other words, restriction of composition on $\sqcup_{B \in \text{Ob}(\mathbf{C})} \text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(B, C)$ maps into $\text{Hom}_{\mathbf{C}}(A, C)$. Hence we can write:

$$c : \sqcup_{A,B,C \in \text{Ob}(\mathbf{C})} \text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(B, C) \rightarrow \sqcup_{A,C \in \text{Ob}(\mathbf{C})} \text{Hom}_{\mathbf{C}}(A, C)$$

for the function composition, and require:

$$c(\sqcup_{B \in \text{Ob}(\mathbf{C})} \text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(B, C)) \subseteq \text{Hom}_{\mathbf{C}}(A, C)$$

It is of course assumed that $\text{Hom}_{\mathbf{C}}(A, B) \cap \text{Hom}_{\mathbf{C}}(C, D) = \emptyset$ whenever $A \neq C$ or $B \neq D$,

which is why disjoint union is utilized.

Now given a category, one can construct a category called its opposite by reversing morphisms:

Definition 2 *The **opposite category** to a category $\mathbf{C}$ is the category whose objects are the same as the objects of $\mathbf{C}$, but the morphisms of the opposite category are morphisms of the first category $\mathbf{C}$ in reverse direction. This means that the morphisms from A into B of the opposite category are the morphisms from B into A in $\mathbf{C}$. Composition is also defined by reversing the order. One denotes the category opposite to a category $\mathbf{C}$ by $\mathbf{C}^{\circ}$.*

*In category theory when one uses the term **dually**, unless otherwise stated, one means that one is making the dual of a statement in the opposite category. One may attach the prefix co- to denote this.*

Also of relevance, is the notion of a subcategory, which basically denotes a category being contained in another.

Definition 3 *A category $\mathbf{C}'$ is called a **subcategory** of a category $\mathbf{C}$ when*

- *the objects of the subcategory are a subcollection of the objects of the initial category, and*
- *the morphisms from an object to another object in the subcategory are also contained in the morphisms of the original category, and*
- *composition is defined in the same fashion, and*
- *identity morphisms be the same.*

*A subcategory is called a **full subcategory** when the morphisms from one object into another object are the same as in the initial category.*

An example of a full subcategory is the category of abelian groups as a subcategory of the category of groups.

An example of a subcategory that is not full is the category of differentiable manifolds as a subcategory of topological spaces.

Another example of a subcategory that is not full is the category of (commutative) rings as a subcategory of abelian groups, by forgetting the multiplication of the ring. Every ring homomorphism is also an abelian group homomorphism with respect to addition of the ring. However not every group homomorphism is a ring homomorphism, as exemplified by the multiplication by an integer, which is a group homomorphism of the additive abelian group of the integers.

Definition 4 *An equivalence relation on morphisms of a category is compatible with composition when two morphisms being equivalent implies that morphisms obtained by precomposition or postcomposition by another morphism are also equivalent. Formally, if $f \sim g$ then $u \circ f \sim u \circ g$ and $f \circ v \sim g \circ v$. Only morphisms with same source and target can be equivalent.*

Lemma 1 *An equivalence relation on morphisms of a category compatible with composition of morphisms allows one to construct a quotient category, with the same collection of objects, and morphisms determined by equivalence classes of morphisms.*

After defining what a category is, one tries to adopt the notions existing in set theory to this new setting. Properties of functions such as being injective, surjective, bijective, inverse have corresponding notions for morphisms with some differences from the notions in set theory, so that one should not think that this is nothing new, nor should one think that it is unrelated to set theory.

Recall that in set theory, a function from product of two sets into a set, for each element of either of the sets forming the product in the domain, defines a function from the other set in the product into the third set. Formally if $f : A \times B \rightarrow C$ is a function, and $a \in A$ and $b \in B$ then $f_a : B \rightarrow C$ is the function defined by $f_a(y) = f(a, y)$ and $f^b : A \rightarrow C$ is the function defined by $f^b(x) = f(x, b)$. This notion can be utilized with the composition function $c_{A,B,C} : \text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(B, C) \rightarrow \text{Hom}_{\mathbf{C}}(A, C)$ to define the functions precomposition

$$\text{precomp}_f : \text{Hom}_{\mathbf{C}}(B, C) \rightarrow \text{Hom}_{\mathbf{C}}(A, C) \quad (2.9)$$

and postcomposition

$$\text{postcomp}_g : \text{Hom}_{\mathbf{C}}(A, B) \rightarrow \text{Hom}_{\mathbf{C}}(A, C)$$

when $f \in \text{Hom}_{\mathbf{C}}(A, B)$ and $g \in \text{Hom}_{\mathbf{C}}(B, C)$ defined by

$$\text{precomp}_f(u) = c_{A,B,C}(f, u) = u \circ f$$

and

$$\text{postcomp}_g(v) = c_{A,B,C}(v, g) = g \circ v$$

Note that condition of associativity can be expressed as commutativity of precomposition and post composition. In other words one can define

Definition 5 *A collection of functions*

$$\{c_{A,B,C} : \text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(B, C) \rightarrow \text{Hom}_{\mathbf{C}}(A, C) \mid A, B, C \in \text{Ob}(\mathbf{C})\} \quad (2.10)$$

for any three objects A, B, C in a collection $\mathbf{C}$ with an assignment of set of morphisms (for each pair of objects in $\mathbf{C}$) is said to be associative at $g : B \rightarrow C$ if for all $h \in \text{Hom}_{\mathbf{C}}(A, B)$ and $f \in \text{Hom}_{\mathbf{C}}(B, C)$,

$$\text{precomp}_h \circ \text{postcomp}_f(g) = \text{postcomp}_f \circ \text{precomp}_h(g)$$

It is said to be associative if it is associate at any morphism.

Note that a morphism $g : B \rightarrow C$ under an existing composition law defines two functions

$$\text{prepost}_g : \text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(C, D) \rightarrow \text{Hom}_{\mathbf{C}}(A, D) \quad (2.11)$$

defined by

$$\text{prepost}_g(f, h) = h \circ (g \circ f) = \text{postcomp}_h \circ \text{precomp}_f(g) = c(c(f, g), h) \quad (2.12)$$

$$\text{postpre}_g : \text{Hom}_{\mathbf{C}}(C, D) \times \text{Hom}_{\mathbf{C}}(A, B) \rightarrow \text{Hom}_{\mathbf{C}}(A, D) \quad (2.13)$$

$$\text{postpre}_g(h, f) = (h \circ g) \circ f = \text{precomp}_f \circ \text{postcomp}_h(g) = c(f, c(g, h)) \quad (2.14)$$

Note that if a collection of morphism composition functions is associative at a morphism $g : B \rightarrow C$, then the two functions defined above are identical.

One then may inquire if / when this function is surjective on a category.

Lemma 2 *Postcomposition in opposite category is precomposition, and precomposition in opposite category is postcomposition.*

Definition 6 *A morphism $f : B \rightarrow C$ is said to be a monomorphism if for all objects A , the function $\text{postcomp}_f : \text{Hom}_{\mathbf{C}}(A, B) \rightarrow \text{Hom}_{\mathbf{C}}(A, C)$ is injective, i.e. $f \circ x = f \circ y$ implies $x = y$. A monomorphism is sometimes called an injective morphism.*

Let $\{\cdot\}$ be a set with a single element, and $\iota_x : \{\cdot\} \rightarrow A$ for $x \in A$ be the embedding of the singleton in A as x . Note that $f \circ \iota_x = f \circ \iota_y$ is equivalent to $f(x) = f(y)$. If f is a monomorphism, then $\iota_x = \iota_y$, which is equivalent to $x = y$. Hence monomorphisms in the category on a collection of sets are injective functions.

Now for any pair of functions $u, v : A \rightarrow B$ and for any pair of elements $x, y \in A$, if $f \circ u = f \circ v$ then $(f \circ u) \circ \iota_x = (f \circ v) \circ \iota_x$. But associativity of composition implies $f \circ (u \circ \iota_x) = f \circ (v \circ \iota_x)$. In set theory this means $f(u(x)) = f(v(x))$, since $u \circ \iota_x = u(x)$, for all $x \in A$. If f is an injective function, then $u(x) = v(x)$ for all $x \in A$. Hence $u = v$. In other words we have shown that if f is an injective function, then it is a monomorphism in the category on a collection of sets.

So in the category of sets, where morphisms are functions, being a monomorphism coincides with being an injective function.

Definition 7 *A morphism $f : A \rightarrow B$ is said to be an epimorphism if the functions $\text{precomp}_f : \text{Hom}_{\mathbf{C}}(B, C) \rightarrow \text{Hom}_{\mathbf{C}}(A, C)$ for all objects C are injective, i.e. for $x, y \in \text{Hom}_{\mathbf{C}}(B, C)$, $x \circ f = y \circ f$ implies $x = y$. An epimorphism is sometimes called a surjective morphism.*

Now define the indicator function $\chi_f = \chi_{\text{im}(f)} : B \rightarrow \{0, 1\}$ by

$$\chi_f(y) = \chi_{\text{im}(f)}(y) = \begin{cases} 1 & \text{if } \exists x \in A \text{ such that } f(x) = y \\ 0 & \text{otherwise} \end{cases} \quad (2.15)$$

Define $1 : B \rightarrow \{0, 1\}$ as the function $1(y) = 1$ for all $y \in B$. Note that $\chi_f \circ f = 1 \circ f$ always, but f is surjective if and only if $\chi_f = 1$.

Stating this carefully, if f is not a surjective function, then there exists $y \in B$ such that $f(x) \neq y$ for any $x \in A$. Therefore $\chi_f(y) = 0$, hence $\chi_f \neq 1$. On the other hand $\chi_f \circ f = 1 = 1 \circ f$ always. Hence f is not an epimorphism.

If f is not an epimorphism, then there exist functions u and v such that $u \circ f = v \circ f$ but $u \neq v$. Now let $y \in B$ be such that $u(y) \neq v(y)$. Such a y exists since $u \neq v$. If there existed $x \in A$ such that $f(x) = y$ then we would have $u(f(x)) = v(f(x))$ by definition of composition of functions. But by assumption $u(y) \neq v(y)$ and $y = f(x)$. Hence there does not exist $x \in A$ such that $f(x) = y$. In other words f is not a surjective function.

So in any category consisting of a collection of sets where morphisms are all possible functions from any of the sets in the collection into any other, the notion of an epimorphism and a surjective function coincide as well.

Lemma 3 *A morphism is a monomorphism if and only if the corresponding morphism in the opposite category is an epimorphism.*

Lemma 4 *The composition of two monomorphisms is a monomorphism and the composition of two epimorphisms is an epimorphism.*

If $f : A \rightarrow B$ and $g : B \rightarrow C$ are monomorphisms, and $u, v : X \rightarrow A$ are any two morphisms such that $(g \circ f) \circ u = (g \circ f) \circ v$, then by associativity of composition this implies that $g \circ (f \circ u) = g \circ (f \circ v)$. Since g is a monomorphism $f \circ u = f \circ v$, and since f is a monomorphism $u = v$. Hence $g \circ f$ is a monomorphism. Since an epimorphism is a monomorphism of the opposite category, composition of two epimorphisms is also an epimorphism.

Lemma 5 *If $a = a' \circ b$ and a is a monomorphism, then so is b . Dually, if $a = b \circ a'$ and a is an epimorphism, then so is b .*

If $b \circ u = b \circ v$ then $a \circ u = (a' \circ b) \circ u = a' \circ (b \circ u) = a' \circ (b \circ v) = (a' \circ b) \circ v = a \circ v$. Since a is a monomorphism $u = v$. Dual statement follows because an epimorphism is a monomorphism of opposite category.

Definition 8 *A morphism that is both a monomorphism and an epimorphism is called a bijection.*

Definition 9 *When a morphism $f : A \rightarrow B$ has a left inverse, i.e. when there is a morphism $r_f : B \rightarrow A$ such that $r_f \circ f = \text{id}_A$, r_f is called a retraction of f .*

Here note that in the category on a collection of sets, where morphisms are functions, set inclusions are retractions. If $\iota : U \rightarrow V$ is an inclusion of sets, any function $r_f : V \rightarrow U$ such that $r_f(u) = u$ for all $u \in U \subseteq V$, is a retraction.

Note that if f has a left inverse, then it is necessarily a monomorphism, because if $f \circ u = f \circ v$ then one can apply r_f on the left to conclude that $u = v$.

Definition 10 *When a morphism $f : A \rightarrow B$ has a right inverse, i.e. when there is a morphism $s_f : B \rightarrow A$ such that $f \circ s_f = \text{id}_B$, s is called a coretraction or section of f .*

In the category on a collection of sets where morphisms are functions, surjective functions always have a section, assuming axiom of choice. For a surjective function $f : A \rightarrow B$, if one defines an equivalence relation on the domain of f by $x \sim_f y$ if and only if $f(x) = f(y)$, then $A / \sim_f$ is isomorphic as a set to B . Isomorphic as a set means that there is a one to one correspondence or function between the set of equivalence classes of A under the equivalence relation $\sim_f$ and the set B . A section is a selection or set of representatives for each equivalence class.

Note that if f has a right inverse, then it is necessarily an epimorphism, since if $u \circ f = v \circ f$ then one can apply s on the right to conclude that $u = v$.

Remark, although in the category of sets a monomorphism necessarily has a left inverse, constructed by mapping anything outside the image to any fixed element for example, and an epimorphism necessarily has a right inverse, which requires the axiom of choice, it is not true in general that a monomorphism has a left inverse and an epimorphism has a right inverse. For example one can construct a category with two objects, and a single

morphism from one into the other. This morphism has neither a left nor a right inverse, but is a monomorphism and epimorphism, vacuously. Note that in this category if A and B are the two objects, then $\text{Hom}(A, A) = \{\text{id}_A\}$, $\text{Hom}(B, B) = \{\text{id}_B\}$, $\text{Hom}(A, B) = \{f\}$ and $\text{Hom}(B, A) = \{\} = \emptyset$

Definition 11 *If a morphism $f : A \rightarrow B$ has both a left and right inverse, then it is called an isomorphism.*

Note that if $f : A \rightarrow B$ is an isomorphism, then left and right inverse should coincide, because $r_f = r_f \circ \text{id}_B = r_f \circ (f \circ s_f) = (r_f \circ f) \circ s_f = \text{id}_A \circ s_f = s_f$.

An isomorphism is a bijection. But not every bijection is an isomorphism.

In the category of metric spaces, the inclusion of $\mathbb{Q}$ inside $\mathbb{R} = \text{MetComp}(\mathbb{Q}) = \text{TopCl}(\mathbb{Q}, \mathbb{R})$ is a bijection, but not an isometry, where $\text{MetComp}(\cdot)$ is the metric completion of the metric space, obtained by taking as the metric space obtained by taking the quotient of the space of all Cauchy sequences of the metric space by the subspace of null Cauchy sequences, i.e. those converging to zero, and $\text{TopCl}(X, Y, \iota : X \rightarrow Y)$ is the topological closure of topological subspace X of Y (where X is seen as a topological subspace of Y via a continuous embedding/inclusion $\iota : X \rightarrow Y$).

If $f, g : \mathbb{R} \rightarrow X$ are such that $f \circ \iota = g \circ \iota$ where $\iota : \mathbb{Q} \rightarrow \mathbb{R}$, then $f(x) = g(x)$ for every $x \in \mathbb{Q}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$ for every real number y there is a sequence x_n of rational numbers that converges to y . But then $f(y) = f(\lim_{n \rightarrow \infty} x_n) = \lim_{n \rightarrow \infty} f(x_n)$. Hence $f(y) = g(y)$. In other words ι is an epimorphism in the category of metric spaces.

ι is not an isometry, because it does not have a continuous inverse. (At the very least cardinality considerations of the sets in question would not allow that).

Definition 12 *A category is called balanced if every bijection is an isomorphism.*

Category of rings is not balanced by the example of inclusion of integers in rational numbers.

Definition 13 *A morphism $f : A \rightarrow C$ is said to factor through in postcomposition with $g : B \rightarrow C$ if f lies in the image of $\text{postcomp}_g : \text{Hom}_{\mathbf{C}}(A, B) \rightarrow \text{Hom}_{\mathbf{C}}(A, C)$. In other words if there exists a morphism $h : A \rightarrow B$ such that $g \circ h = f$. This is shown with the diagram*

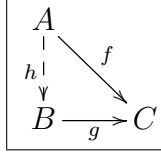


Figure 2.1. f factors through in postcomposition with g

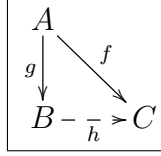


Figure 2.2. f factors through in precomposition with g

Definition 14 If postcomposition with $g : B \rightarrow C$ is surjective then g is called —. If postcomposition is bijective then g is called a terminal object of slice category.

The rationale for the terminology is the following: Slice category of morphisms into a fixed object A of a category $\mathbf{C}$, denoted by $\mathbf{C}_A$, has as its objects elements of $\text{Hom}_{\mathbf{C}}(X, A)$ as X varies over all objects of $\mathbf{C}$. If $\mathbf{C}$ is small, then the object set is $\sqcup_{X \in \text{Ob}(\mathbf{C})} \text{Hom}_{\mathbf{C}}(X, A)$. If $f : X \rightarrow A$ and $g : Y \rightarrow A$ are two objects of the slice category $\mathbf{C}_A$, then $\text{Hom}_{\mathbf{C}_A}(f, g) = \{u \in \text{Hom}_{\mathbf{C}}(X, Y) \mid f = g \circ u\}$. Compositions of morphisms in slice category is defined via composition in $\mathbf{C}$.

Definition 15 An object is called a final or terminal object if from any object in the category, there is a unique morphism into the final object. Dually, an object is called initial if there is a unique morphism from the initial object into any other object of the category.

Definition 16 A morphism $f : A \rightarrow C$ is said to factor through in precomposition with $g : A \rightarrow B$ if f lies in the image of $\text{precomp}_g : \text{Hom}_{\mathbf{C}}(B, C) \rightarrow \text{Hom}_{\mathbf{C}}(A, C)$. In other words if there exists a morphism $h : B \rightarrow C$ such that $h \circ g = f$. This is shown with the diagram

Definition 17 If precomposition with $g : A \rightarrow B$ is surjective, then it is said that every morphism from A into any other object X factors through in precomposition with g . If g is bijective, then g is called an initial object of coslice (comma) category.

Here the morphisms from a fixed object A of a category $\mathbf{C}$ form a category denoted by $\mathbf{C}^A$

$$\begin{array}{ccc}
 A & \xrightarrow{u} & D \\
 \downarrow h & & \uparrow f \\
 B & \xrightarrow{g} & C
 \end{array}$$

Figure 2.3. a morphism u containing a morphism f in a decomposition of compositions, or a morphism u having a decomposition containing f

analogous to slice category.

Definition 18 A morphism $u : A \rightarrow D$ is said to contain $g : B \rightarrow C$ in a decomposition of compositions, or u is said to have a decomposition containing g , if there exist morphisms $h : A \rightarrow B$ $f : C \rightarrow D$ such that $u = f \circ g \circ h$. This is expressed in the diagram:

2.1.2. Subobject

A common notion utilized often in set theory is containment, or that of being a subset, which has various analogues in different branches of mathematics. For example the notion of embedding in topology or differential geometry or in Galois theory. In category theory there is not a priori a relation of containment among objects, but it can be constructed out of the notion of monomorphism. This was carried out in [33] p 123. It is the notion of a subobject, in original *sous-truc*.

Definition 19 A monomorphism $a' : U' \rightarrow V$ is said to majorize or contain another monomorphism $a : U \rightarrow V$ if there exists a morphism $b : U \rightarrow U'$ such that $a = a' \circ b$. Furthermore such a morphism is unique, and is a monomorphism.

Uniqueness of b follows because if $a' \circ b = a' \circ b'$, since a' is a monomorphism, $b = b'$. It has already been proved that if a composition is a monomorphism, then so is the first component of the composition, i.e. the precomposed part.

Lemma 6 The relation of majorizing or containment stated above on morphisms into a fixed object V of a category is a transitive and reflexive relation.

Since $a : U \rightarrow V$ always factorizes as $a = a \circ \text{id}_U$, a majorizes itself. If $a'' : U'' \rightarrow V$ majorizes $a' : U' \rightarrow V$ and a' majorizes $a : U \rightarrow V$ then there exist morphisms $b' : U' \rightarrow$

U'' and $b : U \rightarrow U'$ such that $a = a' \circ b$ and $a' = a'' \circ b'$. Therefore $a = (a'' \circ b') \circ b = a'' \circ (b' \circ b)$. Therefore a'' majorizes a .

Definition 20 Two monomorphisms $a : U \rightarrow V$ and $a' : U' \rightarrow V$ are said to be equivalent if a majorizes a' and a' majorizes a .

Note that this is an equivalence relation. It is reflexive by definition, and by reflexivity of majorization relation. It is symmetric because logical conjunction (and) is. It is transitive by transitivity of majorization and commutation and associativity of conjunction.

Definition 21 A subobject of an object V is the equivalence class of a monomorphism $a : U \rightarrow V$ under the equivalence relation defined above. Alternatively it is a choice of an element of the equivalence class.

Also note the following terminology

Definition 22 A category is said to be locally small at an object A if its subobjects (or equivalence classes of monomorphisms into that object) form a set. [68] p 7.

Lemma 7 If two subobjects $a : U \rightarrow V$ and $a' : U' \rightarrow V$ are equivalent, then the unique monomorphisms $b : U \rightarrow U'$ and $b' : U' \rightarrow U$ such that $a = a' \circ b$ and $a' = a \circ b'$, are in fact isomorphisms.

This follows because, $a \circ \text{id}_U = a = a' \circ b = (a \circ b') \circ b = a \circ (b' \circ b)$. Since a is a monomorphism $b' \circ b = \text{id}_U$ and by same reasoning $b \circ b' = \text{id}_{U'}$.

So now the notion of being a subset in set theory has a category-theoretic analogue, which is a subobject. However a subobject of an object is not only an object, but equivalence class of a monomorphism into that object. In field theory and Galois theory, this notion is something that is already encountered in the notion of an embedding of a field into an extension of that field, which does not have to be unique. $\mathbb{Q}[x]/(x^2 - 2)$ can be embedded by $x \mapsto \sqrt{2}$ or $x \mapsto -\sqrt{2}$ inside any extension of $\mathbb{Q}(\sqrt{2})$, or $\mathbb{Q}[x]/(x^3 - 2)$ can be embedded via $x \mapsto \sqrt[3]{2}$, $x \mapsto \sqrt[3]{2}\zeta_3$ or $x \mapsto \sqrt[3]{2}\zeta_3^2$ inside $\bar{\mathbb{Q}}$. In the last example, two distinct subfields of $\bar{\mathbb{Q}}$ are specified. $\mathbb{Q}(\sqrt[3]{2}\zeta_3)$ is specified twice under two different embeddings.

The field extensions $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt[4]{2}] \subset \bar{\mathbb{Q}}$ can be seen under different nested embeddings as follows:

Let $K = \mathbb{Q}[x]/(x^2 - 2)$, $L = \mathbb{Q}[y]/(y^4 - 2)$, $M = \bar{\mathbb{Q}}$.

Let $\iota^+ : K \rightarrow L$ be defined by $x \mapsto y^2$ and

$\iota^- : K \rightarrow L$ be defined by $x \mapsto -y^2$.

Let $\varrho^+ : L \rightarrow M$ be defined by $y \mapsto \sqrt[4]{2}$ and

$\varrho^- : L \rightarrow M$ be defined by $y \mapsto -\sqrt[4]{2}$,

$\varrho^{i+} : L \rightarrow M$ by $y \mapsto i\sqrt[4]{2}$ and

ϱ^{i-} by $y \mapsto -i\sqrt[4]{2}$.

We have the following list of compositions:

$\sigma^+ : K \rightarrow M$ defined by $x \mapsto \sqrt{2}$ is given by $\varrho^+ \circ \iota^+, \varrho^- \circ \iota^+, \varrho^{i+} \circ \iota^-, \varrho^{i-} \circ \iota^-$

and $\sigma^- : K \rightarrow M$ defined by $x \mapsto -\sqrt{2}$ is given by $\varrho^{i+} \circ \iota^+, \varrho^{i-} \circ \iota^+, \varrho^+ \circ \iota^-, \varrho^- \circ \iota^-$

Here ι^+ and ι^- are the same subobject of L , via the automorphism of K $x \mapsto -x$.

ϱ^+ and ϱ^- are the same subobject of M via the automorphism of L $y \mapsto -y$. Similarly ϱ^{i+} and ϱ^{i-} are the same subobject of M via the automorphism of L $y \mapsto -y$.

σ^+ and σ^- are also the same subobject of M , via the automorphism of K $x \mapsto -x$.

However ϱ^+ and ϱ^{i+} are different subobjects of M .

Another example is the following: one can embed S^1 inside $S^1 \times S^1$ as $\exp(i\theta) \mapsto (\exp(i\theta), 1)$ or $\exp(i\theta) \mapsto (1, \exp(i\theta))$ or $\exp(i\theta) \mapsto (\exp(i\theta), \exp(i\theta))$ or $\exp(i\theta) \mapsto (\exp(\pm i\theta), \exp(\pm i\theta))$, or $\exp(i\theta) \mapsto (\exp(im\theta), \exp(in\theta))$ with m and n being relatively prime. On the other hand, one can embed $\mathbb{R}$ inside $S^1 \times S^1$ as any irrational sloped line through the origin after modding out $\mathbb{R}^2$ by $\mathbb{Z}^2$ to obtain $S^1 \times S^1$. These are all examples of subobjects of $S^1 \times S^1$, both topologically, and geometrically and algebrogeometrically except for the last example where being algebrogeometric fails, unless one makes certain extensions to the meaning of the term. Note that the restriction of the map $z \mapsto (z^m, z^n)$, seen to be from $\mathbb{C}$ into $\mathbb{C}^2$, which is the zero locus of $u^n - v^m$, to S^1 gives the embeddings except the last one. Note also if $u_0^n - v_0^m = 0$ then $(\zeta_n^i u_0)^n - (\zeta_m^j v_0)^m = 0$ as well. In this fashion $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ acts on the embedding $S^1 \hookrightarrow S^1 \times S^1$ given by $(\exp(i\theta) \mapsto \exp(im\theta), \exp(in\theta))$.

In fact we can say the following

$$\mathbb{C}^* \hookrightarrow \mathbb{C}^* \times \mathbb{C}^* \twoheadrightarrow \mathbb{C}^* \quad (2.16)$$

defined by

$$z \mapsto (z^m, z^n) \quad (u, v) \mapsto u^n/v^m$$

is an exact sequence, for m and n relatively prime.

$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ acts on $\mathbb{C}^* \times \mathbb{C}^*$ by $(i, j)(u, v) = (\zeta_n^i u, \zeta_m^j v)$. Furthermore the elements in the same orbit under this action are all mapped to the same element under the last map.

Also $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ both act on $\mathbb{C}^*$ by $z \mapsto \zeta_n^i z$ and $z \mapsto \zeta_m^j z$.

Being relatively prime means that there exist integers a and b so that $am + bn = 1$.

Now consider the joint action of $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ on $\mathbb{C}^*$ defined by $(i, j)z = \zeta_m^i \zeta_n^j z$. The image of the action maps under the first map in the sequence to $(\zeta_n^{mj} z^m, \zeta_m^{in} z^n)$, i.e. the action of (mj, in) on (z^m, z^n) .

What are the orbits of the actions? What are the fibers of the last map? What is their relation?

Here is the argument for demonstrating that the sequence is indeed exact. If $(z_1^m, z_1^n) = (z_2^m, z_2^n)$, then $z_2 = \zeta_m^i z_1$ and $z_2 = \zeta_n^j z_1$ for some integers i, j . But then $\zeta_m^i = \zeta_n^j$. Then $\zeta_n^{mj} = 1$ and $\zeta_m^{ni} = 1$. This can happen if and only if mj is a multiple of n and ni is a multiple of m . Since m and n are relatively prime, j must be a multiple of n and i must be a multiple of m . But in that case $z_2 = z_1$. SO the first map of the sequence is injective.

On the other hand for a nonzero complex number α , one can find a complex number β such that $\beta^n = \alpha$ as one of the roots of the polynomial $z^n - \alpha$. Then $(\beta, 1)$ maps to α under the last map. So the last map of the sequence is surjective.

If $u^n/v^m = 1$, then $u^n - v^m = 0$. Suppose (u_0, v_0) is a nontrivial zero of the polynomial $u^n - v^m$, i.e. $(u_0, v_0) \neq 0$. Now suppose $\alpha^m = u_0$, which is guaranteed to exist by $\mathbb{C}$ being algebraically closed. Now $v_0^m = u_0^n = (\alpha^m)^n = (\alpha^n)^m$. Therefore α^n is a root of the polynomial $z^m - v_0^m$, as well as v_0 . All other roots are of the form $\zeta_m^j \alpha^n$. Therefore $v_0 = \zeta_m^j \alpha^n$, for some integer j . Since there exist integers such that $am + bn = 1$, therefore

$j = jam + jbn$ and $v_0 = \zeta_m^{jbn} \alpha^n = (\zeta_m^{jb} \alpha)^n$. On the other hand since $\alpha^m = u_0$, we have $(\zeta_m^{jb} \alpha)^m = u_0$ as well. In other words, (u_0, v_0) is the image of $\zeta_m^{jb} \alpha$ under the first map of the sequence.

One may want to generalize this example in the following fashion. Suppose we have a map $z \mapsto (f(z), g(z))$ and a map $(u, v) \mapsto F(u)/G(v)$ defined by polynomials or maps from some appropriate family according to the setting so that some condition like exactness is preserved. Note that the first morphism corresponds to parametrizability (by a single parameter) of some object. Whereas lying in the kernel of the second map corresponds to lying on the surface $F(u) = G(v)$. For example if $F(u) = u^2$ and $G(v) = v(v - 1)(v - \alpha)$ then lying in the kernel would correspond to being on an elliptic curve.

Of course there has been some drift from the beginning discussion of reviewing the terms of category theory.

Before returning back to that, there should be some relation of the above example to lens spaces, which I am not delving into right now.

2.1.3. Functors, Natural Transformations

The next concept involves forming assignments or maps from one category into another. This is the notion of a functor which must preserve the commutative diagrams of the source category. This is satisfied by the following

Definition 23 *A functor from one category $\mathbf{C}$ into another category $\mathbf{D}$, (i) assigns objects in the second category to objects of the first category, (ii) assigns morphisms from one object into another in the first category, morphisms from the object assigned to the first object into the object assigned to the second object, (iii) is compatible with composition of morphisms in the corresponding categories (iv) assigns identity morphisms corresponding identity morphism.*

If $F : \mathbf{C} \rightarrow \mathbf{D}$ denotes a functor, then one writes (i) $F(A)$ for the object in $\mathbf{D}$ assigned to the object A in $\mathbf{C}$. (ii) $F(f)$ for the morphism in $\mathbf{D}$ from $F(A)$ into $F(B)$ when f is a morphism from A into B in $\mathbf{C}$. (iii) Compatibility with composition means if $f : A \rightarrow B$ and $g : B \rightarrow C$ are morphisms in $\mathbf{C}$, then $F(g \circ f) = F(g) \circ F(f)$. (iv) Compatibility with identity can be written formally as the condition $F(\text{id}_A) = \text{id}_{F(A)}$.

With the notation for composition one can rewrite compatibility in a more detailed fashion:

$$F(c_{A,B,C}^C(f, g)) = c_{F(A), F(B), F(C)}^D(F(f), F(g)) \quad (2.17)$$

but since this is cumbersome, the first version will be preferred.

The functors defined above are more specifically referred as covariant functors, preserving the order of composition. Contravariant functors reverse order of composition. In other words a contravariant functor from one category into another is a covariant functor from the category opposite to the first one into the second category.

As an example of a covariant functor is abelianization functor that assigns to each group its abelianization, and to each group homomorphism the corresponding abelianization of the group homomorphism. In other words $\text{Ab}(G) = G/[G, G]$. If $f : G \rightarrow H$ is a group homomorphism $\text{Ab}(f)(x[G, G]) = f(x)[H, H]$. Since $f([G, G]) \subset [H, H]$, this is well-defined. (More explicitly for $x, y \in G$, we have $(f(xyx^{-1}y^{-1})) = f(x)f(y)f(x)^{-1}f(y)^{-1}$.) Also it is indeed a homomorphism, since $[G, G]$ is normal in G :

$$x[u, v]x^{-1} = xuvu^{-1}v^{-1}x^{-1} \quad (2.18)$$

$$= xuvx^{-1}(uv)^{-1}(uv)xu^{-1}v^{-1}x^{-1} \quad (2.19)$$

$$= [x, uv]uvxu^{-1}v^{-1}x^{-1} \quad (2.20)$$

$$= [x, uv]u(vx)u^{-1}(vx)^{-1}v xv^{-1}x^{-1} \quad (2.21)$$

$$= [x, uv][u, vx]v xv^{-1}x^{-1} \quad (2.22)$$

$$= [x, uv][u, vx][v, x] \quad (2.23)$$

alternatively

$$x[u, v]x^{-1} = xuvu^{-1}v^{-1}x^{-1} = xuvu^{-1}x^{-1}v^{-1}v xv^{-1}x^{-1} = [xu, v][v, x] \quad (2.24)$$

or more simply:

$$x[u, v]x^{-1} = xuvu^{-1}v^{-1}x^{-1} \quad (2.25)$$

$$= (xux^{-1})(xvx^{-1})(xu^{-1}x^{-1})(xv^{-1}x^{-1}) \quad (2.26)$$

$$= (xux^{-1})(xvx^{-1})(xux^{-1})^{-1}(xvx^{-1})^{-1} \quad (2.27)$$

$$= [xux^{-1}, vxv^{-1}] \quad (2.28)$$

This establishes normality of derived subgroup.

Another example of a functor is the fundamental group in topology, which is a functor from the category of pointed topological spaces into groups, assigning a group homomorphism to continuous functions compatible with or preserving base points. Yet another example would be homology functor.

Cohomology functor on the other hand, is an example of a contravariant functor. A continuous map from one topological space X into another topological space Y induces an abelian group or ring and graded k –algebra homomorphism from the cohomology ring (and graded k –algebra) of topological space Y into that of topological space X .

Yet another example of a functor is the general linear group on a ring or field. If K is a commutative ring or a field, this functor assigns K the group $GL_n(K)$, which can be also seen as n by n invertible matrices with entries in K .

Another example of a functor is the functor that associates to each ring its multiplicative group.

A common example of a functor is the assignment of morphisms, so called Hom–functor. This is contravariant in first variable and covariant in second variable.

Explicitly, $F(X) = \text{Hom}_{\mathbf{C}}(A, X)$ and

$$F(f : X \rightarrow Y)(u : A \rightarrow X) = f \circ u = \text{postcomp}_f(u) \quad (2.29)$$

defines a functor from category $\mathbf{C}$ into the category of sets, and $F(f : X \rightarrow Y) : \text{Hom}_{\mathbf{C}}(A, X) \rightarrow \text{Hom}_{\mathbf{C}}(A, Y)$, i.e. F is covariant.

On the other hand $G(X) = \text{Hom}_{\mathbf{C}}(X, B)$ and

$$G(f : Y \rightarrow X)(u : X \rightarrow B) = u \circ f = \text{precomp}_f(u) \quad (2.30)$$

defines a functor from category $\mathbf{C}$ into the category of sets, and $G(f : Y \rightarrow X) : \text{Hom}_{\mathbf{C}}(X, B) \rightarrow \text{Hom}_{\mathbf{C}}(Y, B)$, i.e. G is contravariant.

Relation of two functors is particularly important. There is the notion of natural transformation from one functor into another to specify this.

A natural transformation from one functor into another, where source and target of both of the functors are identical is given by a collection of morphisms corresponding to each object in the initial category that form commutative diagrams (are compatible with) the images of the morphisms of the initial category under the two functors. Specifically

Definition 24 A natural transformation $\eta : U \rightarrow V$ from functor $U : \mathbf{C} \rightarrow \mathbf{D}$ into the functor $V : \mathbf{C} \rightarrow \mathbf{D}$ assigns to each object X in the category $\mathbf{C}$ a morphism $\eta_X : U(X) \rightarrow V(X)$ in the category $\mathbf{D}$ such that for all morphisms $f : A \rightarrow B$ in $\mathbf{C}$ and all objects A, B in $\mathbf{C}$, one has the commutation of the influence of the functors with the morphisms specified by the natural transformation. Specifically this is expressed in the equation

$$\eta_B \circ U(f) = V(f) \circ \eta_A \quad (2.31)$$

and in the commutative diagram

$$\begin{array}{ccc} U(A) & \xrightarrow{U(f)} & U(B) \\ \eta_A \downarrow & & \downarrow \eta_B \\ V(A) & \xrightarrow{V(f)} & V(B) \end{array}$$

A natural transformation is also referred as a functorial morphism. When the morphisms specified by the natural transformations are isomorphisms, this is called a natural equivalence or functorial isomorphism.

One denotes by $\text{Nat}_{\mathbf{C}, \mathbf{D}}(F, G)$ for $\text{Nat}(F, G)$ natural transformations from functor F into functor G both of which are from category $\mathbf{C}$ into category $\mathbf{D}$. NatEq refers to natural equivalences.

An example of a natural transformation would be abelianization as a natural transformation

from the fundamental group functor into the first homology group functor.

Another example of a natural transformation is the determinant, seen as a natural transformation from the n -dimensional general linear group functor to the multiplicative group of a ring functor. [65] p 16.

Abelianization can be seen as a natural transformation from identity functor to abelianization functor, since the abelianization map is also a group homomorphism, and every abelian group is also a group. [65] p 17.

Lemma 8 *Functors and natural transformations can be composed. This composition is associative.*

2.1.4. Product, Coproduct (Sum) of a Family of Objects

There are slightly different approaches to defining products and coproducts. The one I am following is Grothendieck's in [33]. In set theory, product of two sets itself is a set whose elements are ordered pairs with the first entity in the ordered pair coming from the first set and the second element from the second set. To define an arbitrary product, one may consider a collection of sets indexed by some set. That means an indexing function from the indexing set into a collection of sets. Product of the arbitrary collection can be seen as the collection of all functions from the indexing set into the disjoint union of the collection, such that each function in the collection maps each index into the set assigned by the indexing function to that index. In absence of elements in category theory, and disjoint unions, this definition can not be utilized for category theory. Instead one should really look at only the morphisms in sets to define product. There is always a projection function from the product-set to each set forming the product. To go in the other direction, i.e. constituent sets of the product into the product requires specifying one element from all the other sets forming the product. The latter, i.e. maps from the constituents of a product into the product are not utilizable for category theory.

In category theory, formulation of the product object utilizes the notion of projection. In other words, product should be an object with a morphism to each object forming the product, which will be called a projection morphism.

Furthermore any function from any set B into a product of sets, when composed with

projection, gives functions from set B into the sets forming the product. Furthermore given a collection of functions from a fixed set into the chosen collection of sets forming the product, determines the function from B into the product. This is abstracted into the definition of a product of a collection of objects.

The second property defining a product is that the product be final among all objects that satisfy the first property. If some object also has projection morphisms into the objects “forming” the product, then there is a morphism from that new object into the product object. This property is known as universality. This is taken in various sources as definition of a product. The approach originally taken by Grothendieck is equivalent to this version of the definition. Universality can be deduced from this definition.

Other approaches to defining product and coproduct is through notion of limits and colimits in [1] and through the notion of universal arrows in [65]. Condition of universality is treated in [1].

The approach taken by Grothendieck in [33] is closer to the abstraction of notion of category theory from set theory hence is chosen in this text. However the other notions are also significant for they arise in further generalizations.

Definition 25 For $A \in \text{Ob}(\mathbf{C})$ and $(u_i)_{i \in I}$ a nonempty family of morphisms $u_i : A \rightarrow A_i$ for all $B \in \text{Ob}(\mathbf{C})$ the maps $v \rightarrow u_i v$ of $\text{Hom}_{\mathbf{C}}(B, A)$ in $\text{Hom}_{\mathbf{C}}(B, A_i)$ defines a natural function

$$\text{Hom}_{\mathbf{C}}(B, A) \rightarrow \prod_i \text{Hom}_{\mathbf{C}}(B, A_i) \quad (2.32)$$

One says that u_i define a representation of A as a direct product of A_i if regardless of choice of B the preceding function is bijective.

Lemma 9 If for two families of morphisms (indexed by the same set $i \in I$) $u_i : A \rightarrow A_i$ and $u'_i : A' \rightarrow A'_i$ define a representation of A as direct product of A_i and representation of A' as direct product of A'_i then

- for all families of morphisms $(v_i)_{i \in I}$ with $v_i : A_i \rightarrow A'_i$ there exists a unique morphism $v : A \rightarrow A'$ such that $u'_i v = v_i u_i$ for all i . In other words one has the commutative

diagram

$$\begin{array}{ccc}
 A & \xrightarrow{\quad v \quad} & A' \\
 u_i \downarrow & & \downarrow u'_i \\
 A_i & \xrightarrow{\quad v_i \quad} & A'_i
 \end{array}$$

- If v_i are equivalences (isomorphisms) then so is v .
- If $v_i = I_{A_i}$ then the two objects A, A' represented as products of the family of A_i are canonically isomorphic.

Remark: It need not hold that if v_i are epimorphisms then v is an epimorphism.

Definition 26 For a family $(A_i)_{i \in I}$ of objects of a category $\mathbf{C}$, the object designated by $\prod_{i \in I} A_i$ is said to be a product of the family (A_i) , if there exists a family $(u_i)_{i \in I}$ of morphisms of $\prod_{i \in I} A_i$ in A_i called canonical projections of the product, such that if $v_i : B \rightarrow A_i$ are any family of morphisms from any object B , then there exists a unique morphism $v : B \rightarrow \prod_{i \in I} A_i$ such that $u_i v = v_i$ for all $i \in I$.

- Definition 27**
- $\mathbf{C}$ is a category with finite products if for any two objects (equivalently for any finite and nonempty family of objects) of $\mathbf{C}$ the product of the two objects (of the finite family) exists.
 - $\mathbf{C}$ is a category with infinite products if for any nonempty family of objects of $\mathbf{C}$ product of the family always exists.

Definition 28 If $A = \prod_{i \in I} A_i$ and $B = \prod_{i \in I} B_i$ are two products corresponding to the same set of indices I (with canonical projections u_i and u'_i respectively) then a family of morphisms $v_i : A_i \rightarrow B_i$ define canonically a morphism $v : A \rightarrow B$ called the product of morphisms v_i denoted by $\prod_{i \in I} v_i$ such that $v_i u_i = u'_i v$.

Lemma 10 If v_i above are monomorphisms, then $\prod_{i \in I} v_i$ is also a monomorphisms, but analogous result does not hold for epimorphisms in general. (counter-example: category of sheaves over a fixed topological space.) (explain this example later)

Definition 29 Dual of the preceding considerations allow to define

- the representation of an object A as a sum of a family of objects A_i via the morphisms $u_i : A_i \rightarrow A$ (for all $B \in \text{Ob}(\mathbf{C})$ that the natural function

$$\text{Hom}(A, B) \rightarrow \prod_{i \in I} \text{Hom}(A_i, B) \quad (2.33)$$

is bijective) and also

- the direct sum $\oplus_{i \in I} A_i$ equipped with canonical injections $A_i \rightarrow \oplus_{i \in I} A_i$ (which are not necessarily monomorphisms in spite of their name – explain later), and
- morphism sum of a family of morphisms $u_i : A_i \rightarrow B_i$ denoted by $\oplus_{i \in I} u_i$

Lemma 11 *If u_i are epimorphisms, then so is their morphism sum $\oplus_{i \in I} u_i$.*

Note in comparison to set theory, a coproduct corresponds to a direct sum (as opposed to a direct product) and this notion is used first in modules, where direct sum can be seen as a submodule of the direct product with the additional condition that only finitely many components are nonzero. It can also be utilized for groups with zero replaced by identity of the group. In either case, there is a distinguished element of the parts of a direct sum, namely zero or identity, that allows there to be functions from each member forming the direct sum into the direct sum, by insisting that all other components be zero. These are canonical injections in the definition above. Dual to the notion of a product, instead of considering morphisms from a fixed object into a product, one considers the morphisms from the coproduct into an object, such that when precomposed with the canonical injections, give rise to a family of morphisms from the components of the coproduct into the fixed object. The last property in defining coproduct is the condition of universality, which means that if there is some other object that satisfies same property as the coproduct then there is a morphism from the coproduct into that object. This is referred as coproduct being initial among objects satisfying the first property.

2.1.5. Product of Categories

Lemma 12 *Given two categories one can define the the product of the two categories as the category (rather that what is described in the the following forms a category) whose objects are pairs of objects, the first element of the pair coming from the first category and*

the second from the second category. i.e.

$$\text{Ob}(\mathbf{C} \times \mathbf{D}) = \text{Ob}(\mathbf{C}) \times \text{Ob}(\mathbf{D}). \quad (2.34)$$

(Of course this can be sensibly written only when the objects form a set, otherwise, we stick to the definition of the objects of the product category being pairs.) The morphisms are given by pairs of morphisms.

$$\text{Hom}_{\mathbf{C} \times \mathbf{D}}((a, b), (c, d)) = \text{Hom}_{\mathbf{C}}(a, c) \times \text{Hom}_{\mathbf{D}}(b, d)$$

We are going to assume that this product can be generalized, whenever sensible. As discussed before we are also assuming that pairs of objects can be formed from two collections of objects, and such pairs form a collection of objects themselves.

2.1.6. Multifunctors

Definition 30 A multifunctor is a functor $\prod_i \mathbf{C}_i \times \prod_j \mathbf{C}_j^o \rightarrow \mathbf{D}$ where the functor is covariant in $\mathbf{C}_i$ (or variables with indices i) and contravariant in $\mathbf{C}_j$ (or variables with indices j).

2.1.7. Godement Product, Categories of Functors

Besides previously mentioned sources, this section utilizes the source [69]. Godement product is defined in this source on page 8.

First note that functors from one category into another category form a category, where objects are the functors and morphisms are natural transformations (also called functorial morphisms) from one functor to another. But note now that we have two compositions: composition of natural transformations and composition of functors. These two composition operations are related to each other, which is captured in the definition of Godement product.

Lemma 13 Let $\mathbf{X}$ be a small category (meaning that the collection of its objects form a set), and $\mathbf{Y}$ be another category. Then the (covariant) functors from $\mathbf{X}$ into $\mathbf{Y}$ form a category denoted by $\text{Functors}(\mathbf{X}, \mathbf{Y})$ (or $\text{CovFunctors}(\mathbf{X}, \mathbf{Y})$) or also by $\mathbf{Y}^{\mathbf{X}}$. The contravariant functors also form a category denoted by $\mathbf{Y}^{\mathbf{X}^o}$

Composition of two functors GF with $F : \mathbf{C} \rightarrow \mathbf{C}'$ and $G : \mathbf{C}' \rightarrow \mathbf{C}''$ behaves formally as a bifunctor in relation to its arguments G and F : a natural transformation $G \rightarrow G'$ (or a

natural transformation $F \rightarrow F'$) defines a natural transformation $GF \rightarrow G'F$ (respectively $GF \rightarrow GF'$.)

Lemma 14 A functor $\mathbf{C} \times \mathbf{D} \rightarrow \mathbf{E}$ defines a functor $\mathbf{C} \rightarrow \text{Functors}(\mathbf{D}, \mathbf{E})$ and a functor $\mathbf{D} \rightarrow \text{Functors}(\mathbf{C}, \mathbf{E})$ and vice versa (whenever $\mathbf{C}$ and $\mathbf{D}$ are small categories.)

Note the above can be expressed as

$$\mathbf{E}^{\mathbf{C} \times \mathbf{D}} \cong (\mathbf{E}^{\mathbf{D}})^{\mathbf{C}} \cong (\mathbf{E}^{\mathbf{C}})^{\mathbf{D}} \quad (2.35)$$

Definition 31 If $T : \mathbf{A} \rightarrow \mathbf{B}$ and $V : \mathbf{D} \rightarrow \mathbf{C}$ are functors, where $\mathbf{C}$ and $\mathbf{D}$ are small categories, then there is an induced functor

$$T^V : \mathbf{A}^{\mathbf{C}} \rightarrow \mathbf{B}^{\mathbf{D}} \quad (2.36)$$

defined by

$$T^V(F) = T(F(V))$$

on objects which are functors F and

$$T^V(\phi)_X = T(\phi_{V(X)})$$

on morphisms (natural transformations) $\phi \in \text{Nat}_{\mathbf{C}, \mathbf{A}}(F, G)$, for objects $X \in \text{Ob} \mathbf{D}$, where $\phi_{V(X)} \in \text{Hom}_{\mathbf{A}}(FV(X), GV(X))$, and $T^V(\phi) \in \text{Nat}_{\mathbf{D}, \mathbf{B}}(T^V(F), T^V(G))$.

Definition 32 Godement product of two natural transformations $\alpha : F \rightarrow F'$ and $\beta : G \rightarrow G'$ where $F, F' : \mathbf{A} \rightarrow \mathbf{B}$ and $G, G' : \mathbf{B} \rightarrow \mathbf{C}$ is the natural transformation denoted by $\alpha \cdot \beta : GF \rightarrow G'F'$ whose value at an object $A \in \text{Ob}(\mathbf{A})$ is given by either of the compositions in the following commutative diagram.

$$\begin{array}{ccc} GF(A) & \xrightarrow{\beta_{F(A)}} & G'F(A) \\ \downarrow G(\alpha_A) & & \downarrow G'(\alpha_A) \\ GF'(A) & \xrightarrow{\beta_{F'(A)}} & G'F'(A) \end{array}$$

(Note commutativity of the diagram follows from β being a natural transformation, and $\alpha_A \in \text{Hom}(F(A), F'(A))$. A morphism $f : A \rightarrow A'$ induces a commutative cube from

which it follows that $\alpha \cdot \beta$ is indeed a natural transformation.

$$\begin{array}{ccccc}
 & GF(A) & \xrightarrow{\beta_{F(A)}} & G'F(A) & \\
 GF(f) \swarrow & \downarrow & & \swarrow G'F(f) & \\
 GF(A') & \xrightarrow{\beta_{F(A')}} & G'F(A') & & \\
 \downarrow G(\alpha_{A'}) & \downarrow G(\alpha_A) & & \downarrow G'(\alpha_{A'}) & \downarrow G'(\alpha_A) \\
 GF'(A) & \xrightarrow{\beta_{F'(A)}} & G'F'(A) & & \\
 GF'(f) \swarrow & \downarrow & & \swarrow G'F'(f) & \\
 GF'(A') & \xrightarrow{\beta_{F'(A')}} & G'F'(A') & &
 \end{array}$$

We can isolate the square

$$\begin{array}{ccc}
 GF(A) & \xrightarrow{(\alpha \cdot \beta)_A} & G'F'(A) \\
 GF(f) \downarrow & & \downarrow G'F'(f) \\
 GF(A') & \xrightarrow{(\alpha \cdot \beta)_{A'}} & G'F'(A')
 \end{array}$$

where

$$(\alpha \cdot \beta)_A = G'(\alpha_A)\beta_{F(A)} = \beta_{F'(A)}G(\alpha_A) \quad (2.37)$$

Lemma 15 *Godement product satisfies*

- $1_A \cdot \alpha = \alpha = \alpha \cdot 1_B$
- *It is associative*
- $1_F \cdot 1_G = 1_{GF}$
- $(\alpha\alpha') \cdot (\beta\beta') = (\alpha \cdot \beta)(\alpha' \cdot \beta')$ (*compatibility with composition of natural transformations*)

Remark:

1_A denotes the identity natural transformation from the identity functor to the identity functor of $\mathbf{A}$. (Identity functor assigns each object and each morphism itself).

1_F is the identity natural transformation between F and itself, assigning identity morphism on the object that the functor F maps each object to. In other words, $(1_F)_X = 1_{F(X)}$, for each object X of the category $\mathbf{A}$ where $F : \mathbf{A} \rightarrow \mathbf{B}$ is a functor.

Compatibility of composition of natural transformations with Godement product follows from commutative diagram argument.

Remark on 2-categories: [from [69]] A 2-category is defined as a category whose morphism sets also form a category, and if we denote by $\cdot$ composition of morphisms in the category and by $\perp$ composition of morphisms of morphisms of the category, then

$$(\alpha \perp \alpha') \cdot (\beta \perp \beta') = (\alpha \cdot \beta) \perp (\alpha' \cdot \beta'). \quad (2.38)$$

Alternatively it may be required instead that composition of the category is a functor. In this sense, when we have a collection of categories forming a category, whose objects are categories whose morphisms are functors, and the collection of functors from a fixed category into another fixed category form a category, whose objects are functors, whose morphisms are natural transformations, then this is a 2-category.

2.1.8. Equivalence of Categories

In relating two categories to each other if there is a functor from first category into the second, and another functor from second category to the first such that the compositions yield identity functors of each category then the categories are said to be isomorphic. However there is a looser term that describes similarity of two categories, that is provided by natural equivalence. This notion is called an equivalence of categories. There are several approaches to defining an equivalence of categories. The one below is the definition given in [33].

Definition 33 *An equivalence of a category $\mathbf{C}$ with a category $\mathbf{C}'$ is the system (F, G, ϕ, ψ) formed of covariant functors*

$$F : \mathbf{C} \rightarrow \mathbf{C}' \quad G : \mathbf{C}' \rightarrow \mathbf{C} \quad (2.39)$$

and natural transformations which are natural equivalences

$$\phi : 1_{\mathbf{C}} \rightarrow GF \quad \psi : 1_{\mathbf{C}'} \rightarrow FG$$

where $1_{\mathbf{C}}$ and $1_{\mathbf{C}'}$ are identity functors of $\mathbf{C}$ and $\mathbf{C}'$ respectively, such that for all $A \in \text{Ob}\mathbf{C}$ and $A' \in \text{Ob}\mathbf{C}'$, the compositions are identities of $F(A)$ and $G(A')$ respectively. Two categories are equivalent if there exists an equivalence between these categories.

$$F(A) \xrightarrow{F(\phi_A)} FGF(A) \xrightarrow{\psi_{F(A)}^{-1}} F(A)$$

Figure 2.4. Category equivalence related diagram 1

$$G(A') \xrightarrow{G(\psi_{A'})} GFG(A') \xrightarrow{\phi_{G(A')}^{-1}} G(A')$$

Figure 2.5. Category equivalence related diagram 2

Remark. For all pairs A, B of objects of $\mathbf{C}$ the function $f \mapsto F(f)$ of $\text{Hom}_{\mathbf{C}}(A, B)$ in $\text{Hom}_{\mathbf{C}'}(F(A), F(B))$ is an injection. If $F(f) = F(g)$ then $GF(f) = GF(g)$. But $f = \phi_B^{-1} \circ GF(f) \circ \phi_A = \phi_B^{-1} \circ GF(g) \circ \phi_A = g$.

The function $g \mapsto G(g)$ of $\text{Hom}_{\mathbf{C}'}(F(A), F(B))$ into $\text{Hom}_{\mathbf{C}}(GF(A), GF(B))$ is like an inverse of the previous function, in the following sense: $\text{Hom}_{\mathbf{C}}(GF(A), GF(B))$ is identified with $\text{Hom}_{\mathbf{C}}(A, B)$ by isomorphisms $\phi_A : A \rightarrow GF(A)$ and $\phi_B : B \rightarrow GF(B)$.

Then in case $g = F(f)$ we have $G(g) = GF(f)$ and $\phi_B^{-1} \circ G(g) \circ \phi_A = f$.

On the other hand for $g \in \text{Hom}_{\mathbf{C}'}(FA, FB)$, $FG(g) = \psi_{FB} \circ g \circ \psi_{FA}^{-1}$ i.e.

$$g = \psi_{FB}^{-1} \circ FG(g) \circ \psi_{FA} \quad (2.40)$$

and by assumption $\psi_{FX} = F(\phi_X)$, so

$$g = F(\phi_B^{-1} \circ G(g) \circ \phi_A)$$

, proving that F is surjective on morphisms.

Lemma 16 *Equivalences between categories can be composed just like functors.*

Remark: Isomorphism of categories is stricter than equivalence. In order to serve as an example consider the category formed from a nonempty set, whose morphism sets consist of single elements. Two such categories are equivalent but not isomorphic unless of same cardinality (i.e. equipotent).

2.1.9. More Category Theory Basics: Faithful, Fully Faithful Functor etc.

Definition 34 • A functor $F : \mathbf{A} \rightarrow \mathbf{B}$ is faithful (fully faithful – pleinement fidèle) if for all pairs of objects $S, T \in \text{Ob}(\mathbf{A})$ the map $u \mapsto F(u)$ from $\text{Hom}_{\mathbf{A}}(S, T)$ into

$\text{Hom}_{\mathbf{B}}(F(S), F(T))$ is injective (respectively bijective.) (Functor is called full, if the maps among morphism sets are surjective for every pair of objects of the target category that are images under F of a pair of objects in the source category. This definition is from [65].)

- One says that F is an equivalence of categories if F is fully faithful, and if all objects $U \in \text{Ob}(\mathbf{B})$ are isomorphic to an object of the form $F(S)$. (This definition is equivalent to the previous definition.)
- If, corresponding to F there exists a functor $G : \mathbf{B} \rightarrow \mathbf{A}$ such that GF is isomorphic (naturally equivalent) to $\text{id}_{\mathbf{A}}$ and FG is isomorphic to $\text{id}_{\mathbf{B}}$, then G is called a quasi-inverse of F .

Lemma 17 The two definitions of equivalence of categories coincide.

Lemma 18 A functor F is an equivalence of categories if and only if F has a quasi-inverse.

Proof. Assume that $F : \mathbf{A} \rightarrow \mathbf{B}$ has a quasi-inverse $G : \mathbf{B} \rightarrow \mathbf{A}$.

For each pair of objects $S, T \in \text{Ob}(\mathbf{A})$ assume for $u, v \in \text{Hom}_{\mathbf{A}}(S, T)$ that $F(u) = F(v)$. Then $GF(u) = GF(v)$. Since GF is isomorphic to $\text{id}_{\mathbf{A}}$ there is a natural equivalence which forms a commutative square with the morphism between S and T being either u or v . Since natural equivalence (evaluated at either S or T) is an isomorphism, this implies that $u = v$. i.e. F is injective on morphism sets. (Explicitly, if η denotes the natural equivalence, then the commutative square is

$$\begin{array}{ccc} S & \xrightarrow{\quad} & T \\ \eta_S \downarrow & & \downarrow \eta_T \\ GF(S) & \xrightarrow{\quad} & GF(T) \end{array} \quad \text{then } u = \eta_T^{-1}GF(u)\eta_S = \eta_T^{-1}GF(v)\eta_S = v.$$

Now let $S' \in \text{Ob}(\mathbf{B})$. We claim that $F(G(S'))$ is isomorphic to S' . Noting that $FG \cong 1_{\mathbf{B}}$ there is a natural equivalence ξ that provides this isomorphism. Hence S' is isomorphic (via $\xi_{S'}$ to $F(G(S'))$).

Now for objects $S', T' \in \text{Ob}(\mathbf{B})$ let $w \in \text{Hom}_{\mathbf{B}}(S', T')$. As we have shown, S' is isomorphic to $FG(S')$ and T' is isomorphic to $FG(T')$

Now $G(w) \in \text{Hom}_{\mathbf{A}}(G(S'), G(T'))$ is mapped by F to something we know to be equivalent to w .

But assuming the definition for full as it appears in Saunders Maclane, we are going to pick up $w \in \text{Hom}_{\mathcal{B}}(F(S), F(T))$. Using the incomplete commutative diagram

$$\begin{array}{ccc} S & \dashrightarrow & T \\ \eta_S \downarrow & & \downarrow \eta_T \\ GF(S) & \xrightarrow{G(w)} & GF(T) \end{array}$$

we infer the existence of a morphism $\tilde{w}$ that makes the diagram commutative, since η is a natural equivalence, hence both η_S and η_T are isomorphisms.

Now note the commutative diagram

$$\begin{array}{ccc} F(S) & \xrightarrow{w} & F(T) \\ \xi_{F(S)} \downarrow & & \downarrow \xi_{F(T)} \\ FGF(S) & \xrightarrow{FGF(w)} & FGF(T) \\ F(\eta_S^{-1}) \downarrow & & \downarrow F(\eta_T^{-1}) \\ F(S) & \xrightarrow{F(\tilde{w})} & F(T) \end{array}$$

Note also that by assumption on equivalence of categories the composition of vertical maps is identity, which proves that $F(\tilde{w}) = w$. (Note the vertical arrows are in some sense reverse of the assumption, but it does not matter. Since they are built from natural equivalences, they can be reversed.)

For the other direction, assuming F is fully faithful, and that every object in target category of F is isomorphic to F of some object in source category, we attempt to construct a quasi-inverse.

Note that if $F(A)$ and $F(B)$ are isomorphic, then since F is full, the isomorphism between them is the image of some morphism say from A to B and the inverse of the isomorphism is also the image of a morphism from B to A . Now composition of these two morphisms taken in either order, is mapped by F to identity on $F(A)$ or $F(B)$. Since F is faithful, then composition of these morphisms is identity on A or B , i.e. there is a unique isomorphism in source category that is mapped to the isomorphism between $F(A)$ and $F(B)$. Hence A and B are also isomorphic. In other words, the so called preimage of each object in target category is unique up to isomorphism. Construct G on objects by selecting (by invoking an axiom of choice type argument if necessary) an object in source category that is mapped to something isomorphic to an object in target category. Now for each morphism between some $F(A)$ and $F(B)$, one can find a morphism between A and B mapped to the initial morphism under F since F is full. On the other hand, since F is faithful, such a morphism

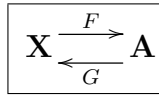


Figure 2.6. Adjunction related diagram

is unique. Hence G is constructed on the image of functor F . (And it is going to preserve compositions by construction, on the objects that are images under F of objects in source category. However it remains to check if G can be well-defined as a functor on objects that are not in the image of F .

First note that for an object in target category that is not in the image of the functor, there is some object in source category that is mapped under F to something isomorphic to that object. Furthermore all objects in source category that are mapped under F to something isomorphic to that object are isomorphic among each other. Now choose for each object in target category, that maps it to something in the image of the functor. Now given a morphism between two objects in target category, the isomorphisms on the domain and codomain of that morphism, carry this morphism to a morphism between image objects of the functor, and there is a unique morphism mapped under F to that morphism, since F is fully faithful. We claim that G we have constructed in this fashion is a quasi-inverse for F (and that it is a functor) and the choice of isomorphisms define the natural equivalence for G to be a quasi-inverse. That it is a functor is almost evident, only taking into consideration that in composition, the use of isomorphism in one direction for target of one morphism and its use in the other direction in the source of the second morphism will cancel each other out. Similarly as a result identity morphism will be carried to identity morphism. That this isomorphism provides the natural equivalence (with the isomorphisms used on the image set being identity isomorphisms) is valid by construction.

Note that the above argument can be broken down and spelled somewhat more easily by use of adjunction.

Definition 35 Let $\mathbf{A}$ and $\mathbf{X}$ be categories. An adjunction from $\mathbf{X}$ to $\mathbf{A}$ is a triple $\langle F, G, \varphi \rangle : \mathbf{X} \rightarrow \mathbf{A}$ where F and G are functors while φ assigns to each pair of objects x an object of $\mathbf{X}$ and a an object of $\mathbf{A}$, a bijection of sets

$$\varphi_{x,a} : \text{Hom}_{\mathbf{A}}(Fx, a) \cong \text{Hom}_{\mathbf{X}}(x, Ga) \quad (2.41)$$

which is natural in x and a . In this case, F is said to be left-adjoint to G and G is a right adjoint for F

In the case of equivalence of categories, note that

$\text{Hom}_{\mathbf{C}'}(F(a), b)$ is mapped to $\text{Hom}_{\mathbf{C}}(GF(a), G(b))$ by the functor G . But $GF(a)$ is isomorphic to a via the natural equivalence ϕ_a^{-1} . Hence we obtain a map to $\text{Hom}_{\mathbf{C}}(a, G(b))$.

Similarly starting with $\text{Hom}_{\mathbf{C}}(a, G(b))$, applying the functor F , this set is mapped to $\text{Hom}_{\mathbf{C}}(F(a), FG(b))$, but $FG(b)$ is isomorphic to b via ψ_b^{-1} .

Hence under an equivalence of categories we have adjunction:

$$\text{Hom}_{\mathbf{C}'}(F(a), b) \cong \text{Hom}_{\mathbf{C}}(a, G(b)). \quad (2.42)$$

2.1.10. Representable Functor, Yoneda Lemma

In this subsection [65] is followed.

Definition 36 A functor is called representable if it is naturally equivalent to the functor which maps each object to the set of morphisms from a fixed object to that object. The fixed object is called the representing object of the functor. In notation: A functor $F : \mathbf{C} \rightarrow \mathbf{Set}$ is representable with representing object $A \in \text{Ob}(\mathbf{C})$ if F is naturally equivalent to $\text{Hom}_{\mathbf{C}}(A, -)$

It is possible to consider also functors naturally equivalent to the functor which assigns each object the set of morphisms from any object to that fixed object.

A useful result related to representable functors is Yoneda's lemma, stated below.

Lemma 19 (Yoneda) There is a set isomorphism between natural transformations from morphisms from a fixed object to a set-valued functor and the image of the fixed object under the set-valued functor. This isomorphism maps each such natural transformation to the image of the identity morphism of the fixed object under the morphism defined by the natural transformation at the fixed object. In notation: If $F : \mathbf{C} \rightarrow \mathbf{Set}$ is a functor from $\mathbf{C}$

and A an object in $\mathbf{C}$ (for $\mathbf{C}$ a category with small hom-sets), there is a bijection

$$\text{Nat}(\text{Hom}_{\mathbf{C}}(A, -), F) \cong F(A) \quad (2.43)$$

which sends each natural transformation $\alpha : \text{Hom}_{\mathbf{C}}(A, -) \rightarrow F$ to $\alpha_A 1_A$, the image of the identity of A in $\mathbf{C}$ under $\alpha_A : \text{Hom}_{\mathbf{C}}(A, A) \rightarrow F(A)$.

Note that $\alpha_B : \text{Hom}_{\mathbf{C}}(A, B) \rightarrow F(B)$ is a morphism in $\mathbf{Set}$ i.e. a function, which maps each morphism from A to B to an element of the set $F(B)$.

Corollary 1 For objects a, b in a category $\mathbf{C}$, each natural transformation $\text{Hom}_{\mathbf{C}}(a, -) \rightarrow \text{Hom}_{\mathbf{C}}(b, -)$ has the form $\text{Hom}_{\mathbf{C}}(h, -)$ for a unique arrow $h : b \rightarrow a$.

2.1.11. Group of Automorphisms of a Functor, and its Action.

Natural transformations are also called morphisms of functors, by considering functors from a fixed category into another category as a category itself. Natural transformations are morphisms of this category. Natural transformations from a morphism to itself, i.e. natural self-transformations, or endomorphisms of functors, can be composed and form a monoid. If one considers natural equivalences from a functor to itself, then these form a group, called the automorphism group of that functor.

Definition 37 Group of automorphisms of a functor is the group of natural (self-) equivalences of that functor. It is denoted by $\text{Aut}(\cdot)$ where $\cdot$ is the name of the functor.

More explicitly, for a functor $F : \mathbf{A} \rightarrow \mathbf{B}$ from category $\mathbf{A}$ to category $\mathbf{B}$, the group of automorphisms of that functor, consists of natural transformations τ which associate to each object $a \in \text{Ob}(\mathbf{A})$ a morphism $\tau_a \in \text{End}_{\mathbf{B}}(F(a))$ that has an inverse $\tau_a^{-1} \in \text{End}_{\mathbf{B}}(F(a))$ such that for all morphisms $f \in \text{Hom}_{\mathbf{A}}(a, b)$ one has

$$F(f) \circ \tau_a = \tau_b \circ F(f) \quad (2.44)$$

i.e.

$$\text{Aut}_{\mathbf{A}, \mathbf{B}}(F) = \text{NatEq}_{\mathbf{A}, \mathbf{B}}(F, F) \quad (2.45)$$

$$= \{ \tau \mid F(f) \circ \tau_a = \tau_b \circ F(f) \ \forall f \in \text{Hom}_{\mathbf{A}}(a, b) \ \forall a, b \in \text{Ob}(\mathbf{A}) \} \quad (2.46)$$

where $\tau_a \in \text{End}_{\mathbf{B}}(F(a))$ for each $a \in \text{Ob}(\mathbf{A})$.

Definition 38 *Action of the group of automorphisms of a functor on morphisms in target category: Group of automorphisms of a functor $F : \mathbf{A} \rightarrow \mathbf{B}$, acts on the morphisms $g \in \text{Hom}_{\mathbf{B}}(F(a), F(b))$ by*

$$\tau g = \tau_b \circ g \circ \tau_a^{-1} \quad (2.47)$$

Remark

$\text{Aut}(F)$ is the subgroup of $\prod_{X \in \text{ob}(\mathbf{A})} \text{Aut}_{\mathbf{B}}(F(X))$ that stabilize elements of each set $F(\text{Hom}_{\mathbf{A}}(a, b))$ for a, b objects in $\mathbf{A}$.

In particular, it is a submonoid of product of centralizers

$$\prod_{X \in \text{ob}(\mathbf{A})} C_{F(\text{End}_{\mathbf{A}}(X))}(\text{End}_{\mathbf{B}}(F(X))) \quad (2.48)$$

and a subgroup of product of centralizers

$$\prod_{X \in \text{ob}(\mathbf{A})} C_{F(\text{Aut}_{\mathbf{A}}(X))}(\text{Aut}_{\mathbf{B}}(F(X)))$$

2.2. AB-CATEGORY, PREADDITIVE CATEGORY, ABELIAN CATEGORY

In addition to previously mentioned sources, another source for abelian categories that is followed is [28].

2.2.1. Preadditive Categories, A –linear Categories

Definition 39 *By a preadditive category is meant a category together with an abelian group structure on each of its hom sets such that composition is bilinear. This is also called an Ab-category.*

A ring (with identity) is a preadditive category with precisely one object, whose morphisms are the ring elements, with composition defined by multiplication of the ring.

Examples. Ab^{Λ} is the category of right Λ –modules where Λ is a ring. Ab^{Λ^*} is the category of left Λ –modules where Λ is a ring, and equivalently denotes the category with a single object, whose endomorphism ring is Λ . Note that natural transformations from one functor

to another (i.e. between two Λ –modules), correspond to abelian group homomorphisms that are compatible with the Λ –action on the abelian groups provided by the functors, hence are Λ –module homomorphisms.

If $\mathbf{A}$ is any category $\mathbf{A}^1$ can be identified with $\mathbf{A}$, (where 1 is the category with a single object and single morphism, which can be seen as the zero ring).

Definition 40 *Let A be a commutative ring with unit. An A –linear category is a category $\mathbf{C}$ such that for every pair of objects X, Y of $\mathbf{C}$, the set of morphisms (arrows) from X to Y $\text{Hom}_{\mathbf{C}}(X, Y)$ is equipped with an A –module structure, which depend functorially on (X, Y) . An A –linear category is also more simply referred as an A –category.*

Remark: It may also be added to the definition that composition of morphisms be A –linear, i.e. an A –module homomorphism.

Note A –linear category is a preadditive category with (abelian group, and ring) morphisms $A \rightarrow \text{End}_{\text{Ab}}(\text{Hom}_{\mathbf{C}}(X, Y))$ for every pair of objects X, Y of $\mathbf{C}$. Note that the endomorphisms of an abelian group form a ring with addition of two endomorphisms being defined by addition of the images of the endomorphisms, and multiplication of endomorphisms being composition of endomorphisms.

Definition 41 *An A –functor from one A –category to another is a functor that is A –linear. On each morphism set which is a A –module, the functor is a A –module homomorphism. ([4] p 7.)*

2.2.2. Kernel, Cokernel, Zero (Null) Object, Image, Coimage, Pullback, Pushout/Pushforward, Product, Sum, Biproduct

Definition 42 *A zero morphism in an additive category is the identity element of the additive abelian group of morphisms. Zero morphism from A to B is denoted by $0_{A,B}$ and the objects are suppressed when there is no confusion.*

Lemma 20 *$0f = 0$ and $g0 = 0$ for all morphisms f, g . Explicitly, if $f : A \rightarrow B$ and $g : B \rightarrow C$ then $0_{B,C}f = 0_{A,C}$ and $g0_{A,B} = 0_{A,C}$*

Note that $0f = 0f + 0 = 0f + af - af = (0 + a)f - af = af - af = 0$. Similarly in the other direction.

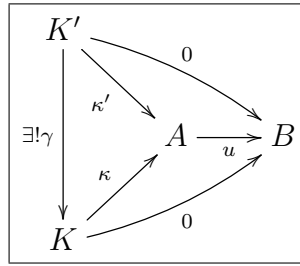


Figure 2.7. Kernel of a morphism

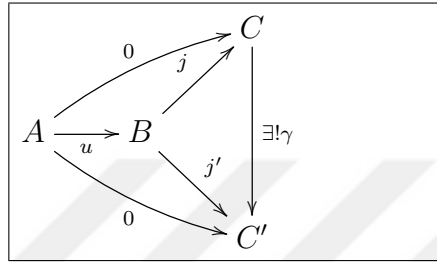


Figure 2.8. Cokernel of a morphism

Definition 43 A kernel of a morphism $u : A \rightarrow B$ in an additive category is a monomorphism $\kappa : K \rightarrow A$ (satisfying $u\kappa = 0$) such that if for a morphism $\kappa' : K' \rightarrow A$ the composition $u\kappa'$ is zero, there is a unique morphism $\gamma : K' \rightarrow K$ such that $\kappa' = \kappa\gamma$. i.e.

(Note alternatively, first one defines difference kernel, and then defines kernel as difference kernel of a morphism and the zero morphism.)

Cokernel is the dual notion to kernel, meaning

Definition 44 A cokernel of a morphism $u : A \rightarrow B$ in an additive category, is an epimorphism $j : B \rightarrow C$ such that $ju = 0$, and there is a unique morphism from cokernel to any epimorphism satisfying the same condition. i.e.

Definition 45 A zero object is an object with a unique morphism from and into any other object. In other words for a zero object the abelian group of morphisms from any object to that object or from that object into any other object is the abelian group with a single element. It is denoted by 0.

Zero object, if it exists, is unique up to isomorphism. If 0 and 0' are both zero objects, then each of the morphism sets $\text{Hom}(0, 0')$ and $\text{Hom}(0', 0)$ and $\text{Hom}(0, 0)$ and $\text{Hom}(0', 0')$

consist of single elements. The composition of the elements in the first two morphism sets in either order, should give the identity element.

In the category of groups or abelian groups, the group with a single element is a zero object.

For completeness, also will include:

Definition 46 *Difference kernel (equalizer) of two morphisms $f, g : A \rightarrow B$ is a monomorphism $\kappa : K \rightarrow A$ such that $f\kappa = g\kappa$, and there is a unique morphism from any other object with a morphism into A satisfying the same condition into the difference kernel, and the morphism factors through the difference kernel via this morphism. In other words if $\kappa' : K' \rightarrow A$ is a monomorphism such that $f\kappa' = g\kappa'$ then there is a unique morphism $\gamma : K' \rightarrow K$ such that $\kappa' = \kappa\gamma$.*

Difference cokernel (coequalizer) is defined similarly.

In additive categories, kernel of a morphism is the difference kernel of that morphism and the zero morphism.

Definition 47 *Given two morphisms $\alpha_1 : A_1 \rightarrow A$ and $\alpha_2 : A_2 \rightarrow A$ with a common target(codomain), a commutative diagram*

$$\begin{array}{ccc} P & \xrightarrow{\beta_2} & A_2 \\ \beta_1 \downarrow & & \downarrow \alpha_2 \\ A_1 & \xrightarrow{\alpha_1} & A \end{array}$$

is called a pullback for α_1 and α_2 if for every pair of morphisms $\beta'_1 : P' \rightarrow A_1$ and $\beta'_2 : P' \rightarrow A_2$ that form a commutative square (i.e. $\alpha_1\beta'_1 = \alpha_2\beta'_2$) there exists a unique morphism $\gamma : P' \rightarrow P$ such that $\beta'_1 = \beta_1\gamma$ and $\beta'_2 = \beta_2\gamma$. Dual of a pullback is called a pushout or pushforward.

Lemma 21 *A pullback is unique up to isomorphism.*

Lemma 22 *If α_1 is a monomorphism, then so is β_2 .*

Lemma 23 *If $(Q, \beta_2 : Q \rightarrow B', \beta_1 : Q \rightarrow I)$ is a pullback of $(B, \alpha_1 : I \rightarrow B, \alpha_2 : B' \rightarrow B)$ and $(P, \gamma_2 : P \rightarrow Q, \gamma_1 : P \rightarrow A)$ is a pullback of $(I, \delta_1 : A \rightarrow I, \delta_2 = \beta_1 : Q \rightarrow I)$ and $\alpha_2 : B' \rightarrow B$ is a monomorphism then the outer rectangle i.e. $(P, \beta_2\gamma_2 : P \rightarrow B', \gamma_1 : P \rightarrow A)$ is a pullback of $(B, \alpha_1 : A \rightarrow B, \alpha_1\alpha_2 : B' \rightarrow B)$ i.e. The diagram below is a*

composition of pullbacks under the condition that $B' \rightarrow B$ is a monomorphism.

$$\begin{array}{ccccc}
 P & \xrightarrow{\gamma_2} & Q & \xrightarrow{\beta_2} & B' \\
 \gamma_1 \downarrow & & \downarrow \beta_1 = \delta_2 & & \downarrow \alpha_2 \\
 A & \xrightarrow{\delta_1} & I & \xrightarrow{\alpha_1} & B
 \end{array}$$

Note it is possible to define intersections and unions via the notion of subobjects, i.e. monomorphisms into an object. Intersection of a collection of objects is a subobject of each of the objects, and is maximal in that property. Union of a collection of objects is an object such that each object in the collection is a subobject of the union, and the union is minimal object with that property.

In the terminology above, the intersection of two subobjects $i_1 : A_1 \rightarrow A$ and $i_2 : A_2 \rightarrow A$ is the pullback of (i_1, i_2) . The union of two objects that contain an object as a subobject, is the pushout of the monomorphisms giving the subobject relation.

Similarly, preimage of a subobject $i : B' \rightarrow B$ of an object B under a morphism $f : A \rightarrow B$ is a subobject $j : A' \rightarrow A$ together with a morphism $\tilde{f} : A' \rightarrow B'$ such that $i\tilde{f} = fj$.

Definition 48 *The image of a morphism $f : A \rightarrow B$ is defined as the smallest object of B which f factors through, i.e. a monomorphism $u : I \rightarrow B$ is the image of f if $f = uf'$ for some $f' : A \rightarrow I$ and if u precedes any other monomorphism into B with same property. Note this is different than the definition of image as cokernel of kernel, which shall appear later.*

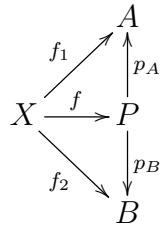
Image of a morphism is the kernel of its cokernel. Coimage of a morphism is the cokernel of its kernel. When image and coimage exist, there is a canonical morphism from coimage to image, which factors each morphism. [33] p 126.

Note image of a subobject $i : A' \rightarrow A$ under a morphism $f : A \rightarrow B$ is the image of fi' .

Product and coproduct (sum) has already been defined, but the definition is repeated here. This version of the definition follows [28].

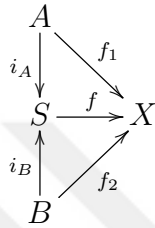
Definition 49 *Product of a pair of objects A and B is an object P together with two morphisms (called projections) $P \xrightarrow{p_A} A$ and $P \xrightarrow{p_B} B$ such that $f_1 : X \rightarrow A$ and $f_2 : X \rightarrow B$ there exists a unique $f : X \rightarrow P$ such that $p_A f = f_1$ and $p_B f = f_2$, i.e. the following*

diagram commutes:



Dual of a product is called a coproduct or a sum. i.e. for

a pair of objects A, B an object P together with two morphisms (called injections) $A \xrightarrow{i_A} S$ and $B \xrightarrow{i_B} S$ such that for any pair of morphisms $f_1 : A \rightarrow X$ and $f_2 : B \rightarrow X$ there exists a morphism $f : S \rightarrow X$ such that $f i_A = f_1$ and $f i_B = f_2$ i.e. the following diagram commutes:



Remark:

Finite sums and products are canonically isomorphic, hence in the definition of an additive and abelian category, this is denoted by the term biproduct, something that is both a product and a sum.

Also for a biproduct in an abelian or additive category $\mathbf{A}$, if $A, B \in \text{Ob } \mathbf{A}$ and $i_A : A \rightarrow A \oplus B$ and $i_B : B \rightarrow A \oplus B$ and $p_A : A \oplus B \rightarrow A$ and $p_B : A \oplus B \rightarrow B$, $A \oplus B \cong A \times B$ then we have

$$i_B p_B + i_A p_A = 1_{A \oplus B} \quad (2.49)$$

and

$$p_A i_A = 1_A, \quad p_B i_B = 1_B$$

. In fact these conditions may be taken as the definition of a biproduct.

A zero (null) object is an object whose identity morphism is the abelian group consisting of only zero, and all zero objects are isomorphic, hence one may denote the zero object by the single letter 0 .

An $\mathbf{A}$ –(linear) functor among two $\mathbf{A}$ –categories that have biproducts, it may additionally be required that the functor is compatible with direct biproduct. In fact this is a consequence. [4], [65].

Lemma 24 *A –linear functors on A –categories preserve biproducts. In fact a functor is additive if and only if it carries binary biproducts to binary biproducts. [65] p 197.*

Note that for an A –linear functor $F : \mathbf{A} \rightarrow \mathbf{B}$ of A –linear categories $\mathbf{A}$ and $\mathbf{B}$, if A and B are objects of $\mathbf{A}$ then $F(i_A)F(p_A) + F(i_B)F(p_B) = 1_{F(A \oplus B)}$ and $F(p_A)F(i_A) = 1_{F(A)}$ and $F(p_B)F(i_B) = 1_{F(B)}$. From here it can be seen that $F(A \oplus B) \cong F(A) \oplus F(B)$, ie. A –linear functors preserve biproducts.

2.2.3. Abelian Category

Recall that:

Ab-category, preadditive category is a category in which

- Hom-sets are additive abelian groups.
- Composition of morphisms is bilinear.

Lemma 25 *An Ab-category (preadditive category) is described by the following*

- *Objects*
- *Function assigning to each ordered pair of objects $\langle a, b \rangle$ an abelian group $A(a, b)$*
- *For each ordered triple of objects $\langle a, b, c \rangle$ morphism of abelian groups called composition*

$$A(b, c) \otimes A(a, b) \rightarrow A(a, c) \quad (2.50)$$

satisfying associative law.

- *For each object a morphism $\mathbb{Z} \rightarrow A(a, a)$ such that unit laws are satisfied in composition.*

Remark: Here note the notational change $A(x, y) = \text{Hom}_A(x, y)$, i.e. the letter denoting the category is also simply used to denote morphisms.

Remark: $A(a, a)$ is not only an abelian group, but also a ring where multiplication is composition. The unit of multiplication is $I_a = 1_a$ the identity morphism of a . The morphism $\mathbb{Z} \rightarrow A(a, a)$ is a ring homomorphism.

Definition 50 *Additive functor (between two Ab-categories) is such that the functor's effect on morphisms $T : A(a, a') \rightarrow B(Ta, Ta')$ is a homomorphism of abelian groups, i.e.*

$$T(f + f') = Tf + Tf' \quad (2.51)$$

Definition 51 *Abelian category is an Ab-category satisfying*

(AB1) *has null object*

(AB2) *has binary biproducts*

(AB3) *every arrow has kernel and cokernel*

(AB4) *Every monic arrow is a kernel and every epi is a cokernel.*

A category satisfying only the first two conditions is called an additive category.

Remark in [33] instead of condition (AB4) there is the following condition:

(AB4') *the canonical morphism from coimage to image is an isomorphism,*

where image is kernel of its cokernel and coimage is cokernel of its kernel. It is stated in [28] p 44 that (AB4) implies (AB4').

If $\mathbf{A}$ is an additive category and $\mathbb{Z}$ is the ring of integers (category with a single object whose endomorphisms is the ring $\mathbb{Z}$), then $\mathbf{A}^{\mathbb{Z}} = \mathbf{A}$. Note that for each functor $F : \mathbb{Z} \rightarrow \mathbf{A}$, there is a map $\mathbb{Z} \cong \text{End}_{\mathbb{Z}}(\cdot) \rightarrow \text{End}_{\mathbf{A}}(F(\cdot))$. Note also that $F(m) = mF(1)$ and $F(1) = \text{id}_{F(\cdot)}$ since 1 is the identity morphism. Note that any (additive) morphism of $\mathbf{A}$ between its objects define a natural transformation between the functors that map the single object of $\mathbb{Z}$ to those objects.

2.2.4. Pseudo-abelian Categories

The following definition appears in [4].

Definition 52 *For a commutative ring with unit A , an A -category is called pseudo-abelian (or karoubian) if all projections (i.e. all endomorphisms $p : X \rightarrow X$ such that $p^2 = p$) have a kernel (and an image).*

Explicitly, for all objects X of the A -category $\mathbf{A}$, and all elements $p \in \text{Hom}_{\mathbf{A}}(X, X)$ such that $p^2 = p$, there exists an object Y of $\mathbf{A}$ and a morphism $f : Y \rightarrow X$ such that f is a kernel

of p . If (C, g) is a kernel for $1 - p$, the morphism $f \amalg g = f \circ \pi_B + g \circ \pi_C : B \oplus C \rightarrow A$ is then an isomorphism. [4] p7. (Here $f \amalg g$ denotes the map from $B \oplus C$ into A induced from the maps f and g by the coproduct.) Note that $f \amalg g$ acts as f on B meaning that $(f \amalg g) \circ i_B = f$, and acts as g on C , i.e. $(f \amalg g) \circ i_C = g$, hence is a monomorphism on B and C .

Note in order to argue that $f \amalg g$ is, say, a monomorphism, one may start asking what the kernel of this morphism should be. (This is the argument for the case when we assume kernels exist in the category.) Note that a kernel for $f \amalg g$ induces a map that, when composed with the projection, gives zero morphism, hence there exists a unique morphism from the kernel to B and by same reason a unique morphism from the kernel to C (this time considering identity minus the projection, which is also a projection). By considering properties of direct sums it can be seen that these morphisms when composed with f and g respectively must give the same morphism which is the zero morphism. Since f and g are themselves kernels, are monomorphisms, so these morphisms must also be zero morphisms, hence the monomorphism defining the kernel is zero, proving that $f \amalg g$ is a monomorphism.

In [4] further reference is made to [78] regarding definition of a karoubian category, and it is remarked that a pseudo-abelian category is often called karoubian. In [78] IV.4.1.2.1 on p 352 definition of karoubian category appears as the difference kernel being representable, and reference is made to 4 Exposé IV Exercice 7.5 [37]: If $p : X \rightarrow X$ is a projection endomorphism of a category $\mathbf{C}$ the kernel of p (rather the difference kernel of (id_X, p) is representable) if and only if the cokernel is. In this case p is said to admit an image and the kernel (which is isomorphic to the cokernel) is called the image of projection.

If one considers say finite dimensional vector spaces, given a projection on a finite-dimensional vector space, the vector space has a direct sum decomposition as the sum of its kernel and image, hence kernel is isomorphic to the cokernel. In the notion of a category, cokernel is dual notion to the kernel, hence kernel is “representable” if and only if cokernel is. (Note that if a monomorphism $\kappa : K \hookrightarrow A$ is kernel of $f : A \rightarrow B$ then in the opposite category, opposite of κ is an epimorphism and is cokernel of opposite of f . $p : X \rightarrow X$ is a projection if and only if its opposite is.) To properly define kernel being representable, one needs to turn morphisms or projections of a category to a category, but if this is carried out, then if kernels exist in a category, then kernel maps each morphism from an object X to

a monomorphism into the object X defined up to isomorphism, hence it is “representable” almost by definition, however to define kernel as a set-valued functor, the category needs to be small, i.e. collection of objects need to be a set, or at the very least, all monomorphisms or monomorphisms into a fixed object need to be a set. Alternatively one needs to understand the term “representable” not only defined for set-valued functors, but in a larger sense. Also kernel would be a contravariant functor.

2.3. RADICAL OF A CATEGORY

This section and the following section follows the articles: [4], [51], [63],[91] in defining notions of ideal of a category, radical of a category and semisimplicity of categories.

If one considers the endomorphisms of an object in a preadditive category, bilinearity of composition under the abelian group operation of the endomorphism set makes the endomorphisms a ring. In order to generalize the notion of an ideal of a ring to this setting one makes the following definition.

Definition 53 *An ideal of a preadditive category $\mathbf{C}$ is a selection, for all objects A, B of $\mathbf{C}$, $\mathbf{I}(A, B)$ of a subgroup of the abelian group $\text{Hom}_{\mathbf{C}}(A, B)$ such that for any other objects X and Y of $\mathbf{C}$ and all $f \in \text{Hom}_{\mathbf{C}}(X, A)$ and $g \in \text{Hom}_{\mathbf{C}}(B, Y)$, $g\mathbf{I}(A, B)f \subset \mathbf{I}(X, Y)$. In other words the subgroup selections are consistent with (closed under) (precomposition- and post-) composition. [51] p 2 p 300. In case the category is A –linear, $\mathbf{I}(A, B)$ is a sub- A –module of $\mathbf{C}(A, B)$. [4] p 9.*

In preadditive categories in which finite direct sums exist, an ideal of the category is determined from ideals $\mathbf{I}_A = \mathbf{I}(A, A)$ for objects A of the category.

Lemma 26 [4] p 13 [51] p 5 *For a preadditive category with direct sums $\mathbf{C}$*

$$\text{rad}(\mathbf{C})(A, B) = \quad (2.52)$$

$$\{f \in \mathbf{Hom}_{\mathbf{C}}(A, B) \mid \forall g \in \text{Hom}_{\mathbf{C}}(B, A), 1_A - gf \text{ is invertible.}\} \quad (2.53)$$

defines an ideal denoted by $\text{rad}(\mathbf{C})$ of $\mathbf{C}$ This ideal is called the radical of $\mathbf{C}$.

Note. If $\mathbf{C}$ is a K –algebra (seen as a K –category with a single object), this is the definition of Jacobson radical, which is the ideal that annihilate all simple right K –modules, or

intersection of all maximal right ideals.

Radical defined in street's article [91] by the condition that $1 - gf$ be a retraction (possess a right inverse). It is stated that this agrees with Jacobson radical with citation given to [47]. It is also proved that:

Lemma 27 *For a morphism $f : A \rightarrow B$, $1 - gf$ is invertible for all $g : B \rightarrow A$ if and only if it is a retraction (possesses a right inverse).*

(Proof assumes that radical is a two-sided ideal, which has also been proved.)

Another radical is given by [30]

Definition 54 *Gabriel's radical is defined by*

$$\text{rad}'(\mathcal{C})(A, B) = \quad (2.54)$$

$$\{f \in \text{Hom}_{\mathcal{C}}(A, B) \mid \forall g \in \text{Hom}_{\mathcal{C}}(B, A) \mid gf \text{ is nilpotent.}\} \quad (2.55)$$

Lemma 28 $\text{rad}'(\mathcal{C}) \subset \text{rad}(\mathcal{C})$ and equality holds if and only if for all $A \in \text{Ob}(\mathcal{C})$, $\text{rad}(\mathcal{C})(A, A)$ is a nilideal (ideal consisting of nilpotent elements).

2.4. SEMISIMPLE CATEGORIES

This section follows [4] except where others are mentioned.

Notation: If $\mathbf{A}$ is an additive category and $A \in \text{Ob}(\mathbf{A})$ then $\mathbf{A}_A = \text{Hom}_{\mathbf{A}}(A, \_)$ is the covariant hom functor represented by A . Similarly $\mathbf{A}_A^* = \text{Hom}_{\mathbf{A}}(\_, A)$ is the contravariant hom functor represented by A .

Definition 55 *A nonzero object A in an abelian category $\mathbf{A}$ is simple if it has no proper, nonzero subobjects, and it is called semisimple if it is a direct sum of simple objects. ([4] Appendice A p 120, [69] p 19.)*

There are several notions of a category of being semisimple, defined in [4], [63],[91]. The definitions in [63] and [91] are weaker than the one in [4] as stated in [4]. The notion is based on or modeled after semisimplicity of rings and modules. Various equivalent conditions which define a category being semisimple are stated in detail in [4] Appendice A. In

particular theorem A.2.10. One needs to define more terms in order to define semisimplicity for categories:

For the following let A be a commutative ring possessing a unit for multiplication, and let A -category mean a category in which morphism sets are A -modules for which composition of morphisms is A -linear.

Let $A - \text{Mod}$ denote the A -linear category of A -modules.

Definition 56 For any A -linear category $\mathbf{A}$, a left $\mathbf{A}$ -module is a A -linear functor $M : \mathbf{A} \rightarrow A - \text{Mod}$. It is said to be finite if $M(A)$ is of finite type over A (finitely generated as a module over A). [4] p 10.

Lemma 29 • $\mathbf{A}$ -modules (or finite $\mathbf{A}$ -modules) form an abelian A -linear category denoted by $\mathbf{A} - \text{Mod}$ (resp. $\mathbf{A} - \text{Mods}$).

- All A -functors $F : \mathbf{A} \rightarrow \mathbf{B}$ induce by composition of A -functors $F^* : \mathbf{B} - \text{Mod} \rightarrow \mathbf{A} - \text{Mod}$ and $F^* : \mathbf{B} - \text{Mods} \rightarrow \mathbf{A} - \text{Mod}$.

Note if $\eta : N_1 \rightarrow N_2$ is a natural transformation, then $F^*(\eta)$ is the natural transformation $\eta_{FX} : F^*N_1 = N_1 \circ F \rightarrow F^*N_2 = N_2 \circ F$.

Definition 57 For a A -category $\mathbf{A}$

- An object is simple if it is nonzero and if it does not have any subobjects other than zero and itself.
- An object is semisimple if it is a direct sum of simple objects.

[4] p 120.

Definition 58 A K -category $\mathbf{A}$ where K is a field, is called semisimple if all left $\mathbf{A}$ -modules are semisimple. [4] p 15.

Barry Mitchell's definition for semisimplicity is the following:

Definition 59 A small additive category $\mathbf{C}$ is left semisimple if $\mathbf{C}_p^*$ (i.e. $\text{Hom}_{\mathbf{C}}(, p)$) is semisimple for all objects $p \in \text{Ob}(\mathbf{C})$ [69] p 19.

Street's article [91] defines semisimple as

Definition 60 “An additive category is called semisimple when it is a local subproduct of a family of simple categories.” [91] p 148

Here local subproduct is defined in the following paragraph:

Definition 61 “Suppose $(\mathcal{A}_\alpha : \alpha \in \Lambda)$ is a family of categories all with the same set of objects.

- The local product of this family is the category $\mathcal{B}$ with the same objects as all the $\mathcal{A}_\alpha$ and with hom groups $\mathcal{B}(A, B)$ given by the product over $\alpha \in \Lambda$ of all the hom groups $\mathcal{A}_\alpha(A, B)$: composition is componentwise. There are local projection functors $P_\alpha : \mathcal{B} \rightarrow \mathcal{A}_\alpha$ which are the identity on objects.
- A category $\mathcal{A}$ is said to be a local subproduct of the family when there exists a faithful functor $\mathcal{A} \rightarrow \mathcal{B}$ which is the identity on objects and whose composite with each P_α is full.

Clearly, $\mathcal{A}$ is a local subproduct of the family $(\mathcal{A}_\alpha : \alpha \in \Lambda)$ iff there exists a family $(\mathcal{K}_\alpha : \alpha \in \Lambda)$ of ideals of $\mathcal{A}$ whose intersection is 0 and for which there are isomorphisms $\mathcal{A}/\mathcal{K}_\alpha \cong \mathcal{A}_\alpha$.”

Here the quotient of categories means that the hom groups are given by the respective quotients of hom groups corresponding to each pair of objects in the category.

In Leduc [63] p 617 a semisimple category is defined as one whose (Kelly) radical is zero.

2.5. LIMIT, COLIMIT, PROJECTIVE AND INJECTIVE LIMIT

This section utilizes formulation of limit and colimit as it appears in [1]. This is also defined through a more involved approach in [65], but the one in Aluffi is more concise.

2.5.1. Colimit and Limit

Definition 62 Let $\mathcal{F} : \mathbf{I} \rightarrow \mathbf{C}$ be a covariant functor. Limit of $\mathcal{F}$ (if it exists) is an object L of $\mathbf{C}$ endowed with morphisms $\lambda_I : L \rightarrow \mathcal{F}(I)$, for all objects I of $\mathbf{I}$ satisfying:

- If $\alpha : I \rightarrow J$ is a morphism in $\mathbf{I}$, then $\lambda_J = \mathcal{F}(\alpha) \circ \lambda_I$:
- L is final with respect to this property: that is if M is another object, endowed with morphisms μ_I , also satisfying the previous requirement, then there exists a unique

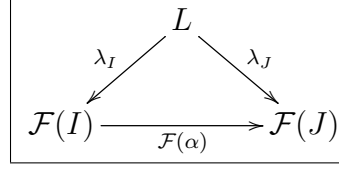
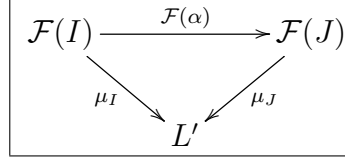
Figure 2.9. Limit of a functor F 

Figure 2.10. Colimit of a covariant functor

morphism $M \rightarrow L$ making all relevant diagrams commute.

Any such datum of M and morphisms is called a cone for $\mathcal{F}$. Therefore the limit of $\mathcal{F}$ is a “universal cone”: it is a final object in the category of cones of $\mathcal{F}$. Limit is also called an inverse or projective limit.

Colimit (direct or injective limit) is the dual notion. i.e.

Definition 63 *Colimit of a covariant functor $\mathcal{F} : \mathbf{I} \rightarrow \mathbf{C}$, is an object L' of $\mathbf{C}$ endowed with morphisms $\mu_I : \mathcal{F}(I) \rightarrow L'$ for all objects I of $\mathbf{I}$ satisfying:*

- *If $\alpha : I \rightarrow J$ is a morphism in $\mathbf{I}$, then $\mu_I = \mu_J \circ \mathcal{F}(\alpha)$:*
- *L' is cofinal / initial with respect to this property: that is if M' is another object, endowed with morphisms λ_I , also satisfying the previous requirement, then there exists a unique morphism $L' \rightarrow M'$ making all relevant diagrams commute.*

2.5.2. Projective and Injective Limits

This subsection utilizes the definitions in [12] and [11] and [26].

Preorder relation, order relation, partial order

Definition 64 • *A preorder relation is a relation that satisfies transitivity and that if $x \leq y$ then $x \leq x$ and $y \leq y$. (i.e. it is reflexive on elements that are related to some other element.)*

- A preorder relation is an order relation if in addition $x \leq y$ and $y \leq x$ implies $x = y$. (i.e. anti-symmetric.)
- An order relation in which any two elements of a set are comparable (i.e. $x \leq y$ or $y \leq x$ is true) is called a total order relation.
- If on every ordered nonempty subset (ordered by the relation on the set) there is a least element, the relation is said to be a well-ordering.
- A partial order relation is a relation that is reflexive (i.e. $x \leq x$ for all elements of the set), anti-symmetric (i.e. if $x \leq y$ and $y \leq x$ then $x = y$) and transitive. (Dummit and Foote)
- An equivalence relation is one that is reflexive, symmetric, and transitive. (Symmetric means $R(x, y)$ implies $R(y, x)$.)

Remark: In Bourbaki, it seems that relation has a meaning more general than relation on a set, which is simply a subset of product of two sets (which are taken equal to each other). Due to this, a preorder relation has the extra condition that reflexive property is confined to the elements that are present in a relation. However, there is a definition of preorder relation on a set, defined later, that requires $x \leq x$ being equivalent to x being an element of the set in consideration (which implies reflexivity on the set of definition). Bourbaki definition of relation is for logical statements Rxy or xRy is a logical statements with terms x and y , which can be replaced with anything (not necessarily restricted to values on a set).

Projective limit (inverse limit)

Definition 65 If $\mathbf{I}$ is a preordered set (a set with a relation that is transitive and reflexive on elements that are present in at least one relation member) and $(A_i)_{i \in \mathbf{I}}$ is a family of sets (or groups or modules) indexed by $\mathbf{I}$ and for all couple (i, j) of indices with $i \leq j$

$$f_{j,i} : A_j \rightarrow A_i, \quad i \leq j \tag{2.56}$$

are morphisms satisfying

- If $i \leq j \leq k$ then $f_{k,i} = f_{j,i} \circ f_{k,j}$
- $f_{i,i} = \text{id}_{A_i}$

then $\mathbf{A} = \varprojlim A_i$ is defined as the subset of $\prod_{i \in \mathbf{I}} A_i$ consisting of those $a \in \prod_{i \in \mathbf{I}} A_i$ such that $\text{pr}_i(a) = f_{j,i}(\text{pr}_j(a))$ where $\text{pr}_i : \prod_{i \in \mathbf{I}} A_i \rightarrow A_i$ are the projection maps.

$$\varprojlim A_i = \{a \in \prod_{i \in \mathbf{I}} A_i \mid \text{pr}_i(a) = f_{j,i}(\text{pr}_j(a)) \forall i \forall j \geq i\} \quad (2.57)$$

An example is $\mathbb{Z}_p$, the ring of p -adic integers with morphisms $r_{i,j} = \mathbb{Z}/p^j\mathbb{Z} \rightarrow \mathbb{Z}/p^i\mathbb{Z}$ for $j \geq i$ being the usual projection maps.

The definition of $\hat{\mathbb{Z}}$ with $r_{m,n} : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ whenever $n|m$, is another example of a projective limit.

Definition of Direct (injective) Limit

Definition 66 A preordered set is directed if for each pair (i, j) of elements of the set, there is an element k of the set such that $k \geq i$ and $k \geq j$.

Definition 67 If $\mathbf{I}$ is a preordered (or partially ordered) set that is directed, and to each index $i \in \mathbf{I}$ corresponds a set or group or module A_i and for each pair $i \leq j$ there exists a morphism $f_{i,j} : A_i \rightarrow A_j$ such that

- If $i \leq j \leq k$ then $f_{i,k} = f_{j,k}f_{i,j}$
- For all $i \in \mathbf{I}$, $f_{i,i} = \text{id}_{A_i}$

then the direct (injective) limit is defined as

$$\varinjlim A_i = \sqcup_{i \in \mathbf{I}} A_i / \sim \quad (2.58)$$

where $a_i \sim a_j$ if there exists $k \in \mathbf{I}$ with $k \geq i$ and $k \geq j$ such that $f_{i,k}(a_i) = f_{j,k}(a_j)$

Relation defining direct limit is an equivalence relation

Clearly $a_i \sim a_i$ since $f_{i,i}(a_i) = a_i$.

If $a_i \sim a_j$ then there exists $k \geq i, j$ such that $f_{i,k}(a_i) = f_{j,k}(a_j)$. Hence $a_j \sim a_i$.

If $a_i \sim a_j$ and $a_j \sim a_k$ then there exists $r \geq i, j$ and $s \geq j, k$ such that $f_{i,r}(a_i) = f_{j,r}(a_j)$ and $f_{j,s}(a_j) = f_{k,s}(a_k)$.

Since $\mathbf{I}$ is a directed set there exists an index $t \geq r, s$ and then

$$f_{i,t}(a_i) = f_{r,t}f_{i,r}(a_i) = f_{r,t}f_{j,r}(a_j) = f_{j,t}(a_j) = f_{s,t}f_{j,s}(a_j) = f_{s,t}f_{k,s}(a_k) = f_{k,t}(a_k) \quad (2.59)$$

This proves that $a_i \sim a_k$. Note that being directed is a necessary assumption here.

Inclusion maps from sets into the injective limit

There are inclusion maps of each A_i in the direct limit, via the inclusion in the disjoint union and the projection to the equivalence classes. Clearly they commute with the morphisms $f_{i,j}$.

Morphisms into a projective limit and morphisms from an injective limit

A morphism $t : x \rightarrow \varprojlim A_i$ determines morphisms $t_i : x \rightarrow A_i$ via composing t with the projection maps $\text{pr}_i : \varprojlim A_i \rightarrow A_i$. If $f_{j,i} : A_j \rightarrow A_i$ for $j \geq i$ are the morphisms defining the projective (inverse) limit, then $t_i = f_{j,i} \circ t_j$, since $t_i = \text{pr}_i \circ t$. Conversely given morphisms $t_i : x \rightarrow A_i$ for each i , they determine a morphism $t : x \rightarrow \varprojlim A_i$ if they satisfy the condition $t_i = f_{j,i} \circ t_j$. (This is the universal property of limit, which as will be proved below, projective limit is a limit of the functor determined by the assignment $i \mapsto A_i$ and $(i \leq j) \mapsto f_{j,i}$.)

A morphism $t : \varinjlim A_i \rightarrow x$ determines morphisms $t_i : A_i \rightarrow x$ via composing t with the inclusion maps $\iota_i : A_i \rightarrow \varinjlim A_i$. If $f_{i,j} : A_i \rightarrow A_j$ for $i \leq j$ are the morphisms defining the injective (direct) limit, then $t_i = t_j \circ f_{i,j}$, since $t_i = t \circ \iota_i$. Conversely given morphisms $t_i : A_i \rightarrow x$ satisfying the condition $t_i = t_j \circ f_{i,j}$, they determine a morphism $t : \varinjlim A_i \rightarrow x$. (This is the universal property of colimit, which as will be proved below, injective limit is a colimit of the functor determined by the assignment $i \mapsto A_i$ and $(i \leq j) \mapsto f_{i,j}$.)

2.5.3. Compatibility of Category-theoretic Definition and Algebraic Definition

In this section the following will be proved:

Lemma 30 *A reflexive and transitive relation on a set I determines a category $\mathbf{I}$ whose objects are elements of the set, and for $a, b \in I$, $\text{Hom}(a, b)$ consists of a single element whenever $a \leq b$, (and empty otherwise). A preorder relation on a set I also determines a category, with the additional modification that $\text{Hom}(a, a)$ always has a single element (the identity of a), or by removing those elements from I that do not enter into any relation.*

- Lemma 31** • *Projective limit of $(A_i, f_{j,i})_{i,j \in I, i \leq j}$ where $A_i \in \text{Ob}(\mathcal{C})$ and $f_{j,i} : A_j \rightarrow A_i$ are morphisms in $\mathcal{C}$ for $j \geq i$ is limit of the contravariant functor $\mathcal{F} : \mathbf{I} \rightarrow \mathcal{C}$ defined by $\mathcal{F}(i) = A_i$ and $\mathcal{F}(i \leq j) = f_{j,i}$.*
- *Injective limit of $(A_i, f_{i,j})_{i,j \in I, i \leq j}$ where $A_i \in \text{Ob}(\mathcal{C})$ and $f_{i,j} : A_i \rightarrow A_j$ are morphisms in $\mathcal{C}$ for $i \leq j$ is colimit of the covariant functor $\mathcal{F} : \mathbf{I} \rightarrow \mathcal{C}$ defined by $\mathcal{F}(i) = A_i$ and $\mathcal{F}(i \leq j) = f_{i,j}$.*

For $\mathcal{C}$ being set, group, ring, R -module. $\varinjlim A_i$ and $\varprojlim A_i$ is a set, group, ring or R -module whenever A_i are.

Note that although limit is defined for a covariant functor, one can define limit of a contravariant functor as the limit of the covariant functor from the opposite category $\mathbf{I}^o$.

If there is a relation on a set that is reflexive and transitive, then there is a category whose objects are elements of the set, and for a, b elements of the set, if $a \leq b$ then there is a unique morphism from a to b , and none otherwise.

(Note a preorder is not enough to define a category on all elements of the set, since it is required that $a \leq a$ so that the hom-set $\text{Hom}(a, a)$ contains an element. However a reflexive preorder is. Also a preorder is enough to define a category on all elements of the set x such that there is an element y with $x \leq y$ or $y \leq x$.)

On the other hand given any category whose objects form a set, one can define a relation on the set by declaring $a \leq b$ whenever $\text{Hom}(a, b)$ is nonempty. Such a relation is necessarily reflexive, since $1_a \in \text{Hom}(a, a)$ from definition of category. Furthermore it is necessarily transitive, since if $\text{Hom}(a, b)$ and $\text{Hom}(b, c)$ are both nonempty, then $\text{Hom}(a, c)$ is definitely nonempty, by composition. Hence it is a preorder relation that is reflexive.

Now assume that $\mathbf{I}$ is a set with a relation that is transitive and reflexive. Consider $\mathbf{I}$ as a category with $\text{Hom}(a, b)$ consisting of a single element if $a \leq b$, and empty otherwise. If there is a preorder relation on $\mathbf{I}$, then enforce $\text{Hom}(a, a)$ to always consist of a single element even if $a \not\leq a$.

When $\mathcal{C}$ is the category of sets, groups, rings, R -modules, etc., consider a covariant/contravariant functor $\mathcal{F} : \mathbf{I} \rightarrow \mathcal{C}$.

This means

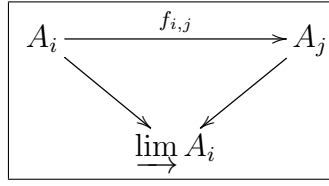


Figure 2.11. Injective/Direct Limit

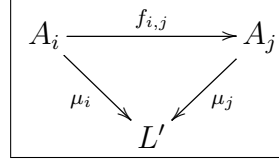


Figure 2.12. Injective/Direct limit, universality

- To each $i \in \mathbf{I}$ corresponds a set, group, ring, R -module, etc. $\mathcal{F}(i) = A_i$.
- Whenever $i \leq j$ in $\mathbf{I}$, there is a morphism of sets, groups, rings, R -modules

$$\mathcal{F}(i \rightarrow j) = f_{i,j} : A_i \rightarrow A_j \quad (2.60)$$

when $\mathcal{F}$ is covariant, and

$$\mathcal{F}(i \rightarrow j) = f_{j,i} : A_j \rightarrow A_i$$

when $\mathcal{F}$ is contravariant

- If $i \leq j \leq k$ then

$$\mathcal{F}(i \rightarrow k) = \mathcal{F}(j \rightarrow k)\mathcal{F}(i \rightarrow j) \quad (2.61)$$

i.e. $f_{i,k} = f_{j,k} \circ f_{i,j}$ when $\mathcal{F}$ is covariant and

$$\mathcal{F}(i \rightarrow k) = \mathcal{F}(i \rightarrow j)\mathcal{F}(j \rightarrow k) \quad (2.62)$$

i.e. $f_{k,i} = f_{j,i} \circ f_{k,j}$ when $\mathcal{F}$ is contravariant

- For all $i \in \mathbf{I}$ since $\text{Hom}(i, i) = \{\text{id}_i\}$, we have $\mathcal{F}(i \rightarrow i) = \text{id}_{\mathcal{F}(i)}$

Now since

whenever $i \leq j$ and if L' is any other set with maps $\mu_i : A_i \rightarrow L'$ such that the diagram below commutes,

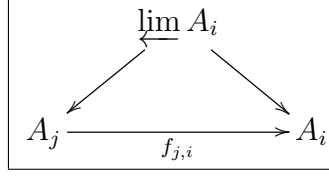


Figure 2.13. Projective/Inverse Limit

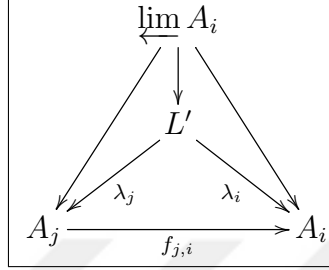


Figure 2.14. Projective/Inverse Limit, universality

then one can define a map

$$\varinjlim A_i \rightarrow L' \quad (2.63)$$

by mapping the equivalence class of a_i in $\varinjlim A_i$ to $\mu_i(a_i)$. This is independent of choice of i . Note that $a_i \sim a_j$ if and only if there exists some $k \geq i, j$ such that $f_{i,k}(a_i) = f_{j,k}(a_j)$. But then

$$\mu_i(a_i) = \mu_k f_{i,k}(a_i) = \mu_k f_{j,k}(a_j) = \mu_j(a_j) \quad (2.64)$$

Hence $\varinjlim A_i$ is indeed the colimit of the functor $\mathcal{F} : \mathbf{I} \rightarrow \mathbf{C}$.

On the other hand if $\mathcal{F}$ is contravariant, then

Similarly if L' is another object in $\mathbf{C}$ with morphisms $\lambda_i : L' \rightarrow A_i$ such that the following diagram is commutative, then one can define a map

$$L' \rightarrow \varprojlim A_i \quad (2.65)$$

by mapping each $x \in L'$ to $a \in \prod_i A_i$ with $\text{pr}_i(a) = \lambda_i(x)$. Clearly $a \in \varprojlim A_i$.

This establishes that $\varprojlim A_i$ is a limit of the contravariant functor $\mathcal{F}$.

Projective/Injective limit acquires necessary algebraic structure

If the sets A_i have an operation, and the maps $f_{i,j}$ or $f_{j,i}$ preserve the operation, then

(i) Projective limit is a subset of the direct product. An operation on the direct product will be defined by the operation on the components. Since the maps $f_{j,i} : A_j \rightarrow A_i$ for $j \geq i$ preserve the operation, if $a, b \in \varprojlim A_i$, then $a + b$ or $a * b$ will also lie in $\varprojlim A_i$. Let's denote the operation by $o(a, b)$ on $\varprojlim A_i$ and operation on A_i by $o_i(-, -)$. Then

$$\text{pr}_i(o(a, b)) = o_i(\text{pr}_i(a), \text{pr}_i(b)) \quad (2.66)$$

$$= o_i(f_{j,i}(\text{pr}_j(a)), f_{j,i}(\text{pr}_j(b))) \quad (2.67)$$

$$= f_{j,i}(o_j(\text{pr}_j(a), \text{pr}_j(b))) \quad (2.68)$$

$$= f_{j,i}(\text{pr}_j(o(a, b))) \quad (2.69)$$

Hence when $a, b \in \varprojlim A_i$ then so is $o(a, b)$.

(ii) Define the operation on the direct (injective) limit as follows: If $a \in \varinjlim A_i$ is the class of $a_i \in A_i$ and $b \in \varinjlim A_i$ is the class of $b_j \in A_j$, then there exists an index k such that $i, j \leq k$. For any such k , define $o(a, b)$ as the class of $o_k(f_{i,k}(a_i), f_{j,k}(b_j))$.

Suppose $a_{i'} \in A_{i'}$ and $b_{j'} \in A_{j'}$ are in the same class as a_i and b_j respectively, then there exist indices $i'' \geq i, i'$ and $j'' \geq j, j'$ such that $f_{i,i''}(a_i) = f_{i',i''}(a_{i'})$ and $f_{j,j''}(b_j) = f_{j',j''}(b_{j'})$. We need to show that for $k' \geq i', j'$, $o_k(f_{i,k}(a_i), f_{j,k}(b_j))$ is in same class as $o_{k'}(f_{i',k'}(a_{i'}), f_{j',k'}(b_{j'}))$.

Let $k'' \geq k, k'$. Then $k'' \geq i, j, i', j'$. We can assume that $k'' \geq i'', j''$ as well. (If not simply

choose a larger index).

$$f_{k,k''} o_k(f_{i,k}(a_i), f_{j,k}(b_j)) = o_{k''}(f_{k,k''} \circ f_{i,k}(a_i), f_{k,k''} \circ f_{j,k}(b_j)) \quad (2.70)$$

$$= o_{k''}(f_{i,k''}(a_i), f_{j,k''}(b_j)) \quad (2.71)$$

$$= o_{k''}(f_{i'',k''} \circ f_{i,i''}(a_i), f_{j'',k''} \circ f_{j,j''}(b_j)) \quad (2.72)$$

$$= o_{k''}(f_{i'',k''} \circ f_{i',i''}(a_{i'}), f_{j'',k''} \circ f_{j',j''}(b_{j'})) \quad (2.73)$$

$$= o_{k''}(f_{i',k''}(a_{i'}), f_{j',k''}(b_{j'})) \quad (2.74)$$

$$= o_{k''}(f_{k',k''} \circ f_{i',k'}(a_{i'}), f_{k',k''} \circ f_{j',k'}(b_{j'})) \quad (2.75)$$

$$= f_{k',k''} o_{k'}(f_{i',k'}(a_{i'}), f_{j',k'}(b_{j'})) \quad (2.76)$$

$$(2.77)$$

This establishes that the operation is well-defined.

Associativity of the operation can be proved via assuming associativity of the operation on each A_i . (Same with commutativity and other properties). The trick is moving to a large enough index.

If $a, b, c \in \varinjlim A_i$ and a is class of $a_i \in A_i$ and b is class of $b_j \in A_j$ and c is class of $c_k \in A_k$ then choose an index $l \geq i, j, k$. Then associativity follows from associativity of operation in A_l .

For showing say distributivity (where three indices will be involved as well), the same argument holds. (When there are two operations, one distributive over the other, as in a ring.)

For demonstrating properties for R -modules, note that in such a case the maps $f_{j,i}$ will be R -module homomorphisms.

2.5.4. When Direct and Inverse Limits are Nonempty

Direct limit is always nonempty, when at least one A_i is nonempty.

Definition 68 A subset A of a preordered set E is cofinal (coinitial) in E if for every $x \in E$ there exists $y \in A$ such that $x \leq y$ (resp. $y \leq x$.)

Lemma 32 Let $(E_\alpha, f_{\beta,\alpha})_{\alpha,\beta \in I, \alpha \leq \beta}$ be an inverse system and $E = \varprojlim E_i$ be the inverse (projective) limit. Suppose that I is directed and has a countable cofinal subset, and $f_{\beta,\alpha}$ are surjective. Then the canonical projections $f_\alpha : E \rightarrow E_\alpha$ are surjective. Hence E is non-empty if none of the E_α are.

Theorem 1 Suppose I is a directed set. Let $\{S_\alpha \mid \alpha \in I\}$ be a set of subsets of the sets E_α for each $\alpha \in I$ satisfying

- (i) Every intersection of sets belonging to S_α belongs to S_α (by considering empty intersection, if necessary)
- (ii) If a set of subsets $\mathfrak{F} \subset S_\alpha$ is such that every finite intersection of sets belonging to $\mathfrak{F}$ is non-empty, then $\cap_{M \in \mathfrak{F}} M$ is non-empty.
- (iii) For each pair of indices α, β such that $\alpha \leq \beta$, and each $x_\alpha \in E_\alpha$ $f_{\beta,\alpha}^{-1}(x_\alpha) \in S_\beta$.
- (iv) For each pair of indices α, β such that $\alpha \leq \beta$ and each $M_\beta \in S_\beta$ $f_{\beta,\alpha}(M_\beta) \in S_\alpha$.

Let $E = \varprojlim E_\alpha$ and $f_\alpha : E \rightarrow E_\alpha$ be canonical mapping. Then

- (a) For each $\alpha \in I$,

$$f_\alpha(E) = \cap_{\beta \geq \alpha} f_{\beta,\alpha}(E_\beta) \quad (2.78)$$

- (b) If E_α is non-empty for each $\alpha \in I$, then E is non-empty.

Sketch of proof of lemma

It suffices to prove the case for $I = \mathbb{N}$, due to existence of a countable cofinal subset. (The coordinates outside the cofinal subset are to be determined from the coordinates in the cofinal subset.)

By using property of being directed, inductively one can form a countable cofinal subset that is increasing. Then one proves surjectivity of f_0 the projection on the first (least) index

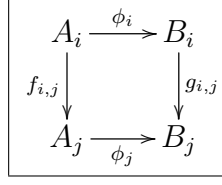


Figure 2.15. Morphism between Two Limits

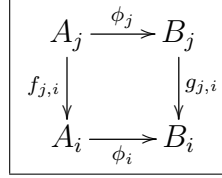


Figure 2.16.

in the countable cofinal subset, by utilizing surjectivity of $f_{\beta,\alpha}$.

Sketch of proof of theorem

This is an application of Zorn's lemma on

$$\{(A_\alpha)_{\alpha \in I} \mid A_\alpha \neq \emptyset, \text{ and } A_\alpha \in S_\alpha \text{ } f_{\beta,\alpha}(A_\beta) \subset A_\alpha \text{ if } \alpha \leq \beta\} \quad (2.79)$$

which is ordered by the relation $(A_\alpha) \leq (A'_\alpha)$ when $A_\alpha \supset A'_\alpha$ for all α . One establishes that for the maximal element (A_α) , A_α should consist of a single element by maximality.

2.5.5. Morphism between two Direct and Projective Limits

Theorem 2 If $A = \varinjlim A_i$ and $B = \varinjlim B_i$ with the morphisms defining the limits being $f_{i,j}$ and $g_{i,j}$ respectively, and there exists morphisms $\phi_i : A_i \rightarrow B_i$ such that then there exists a (unique) morphism $\phi : A \rightarrow B$ such that

$$\begin{array}{ccc} A_i & \xrightarrow{\phi_i} & B_i \\ \iota_i^A \downarrow & & \downarrow \iota_i^B \\ A & \xrightarrow{\phi} & B \end{array}$$

Theorem 3 If $A = \varprojlim A_i$ and $B = \varprojlim B_i$ with the morphisms defining the limits being $f_{j,i}$ and $g_{j,i}$ respectively, and there exists morphisms $\phi_i : A_i \rightarrow B_i$ such that then there exists a

(unique) morphism $\phi : A \rightarrow B$ such that

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \text{pr}_i^A \downarrow & & \downarrow \text{pr}_i^B \\ A_i & \xrightarrow{\phi_i} & B_i \end{array}$$

3. ALGEBRAIC GEOMETRY

Main sources for this section are [39], [16], [95]. This chapter reviews the terminology of algebraic geometry following the cited sources. The basic goal is to define a variety, which can initially be defined as zero set of a polynomial. In order to analyze using techniques of algebra and commutative algebra properties of a geometrically motivated concept, the notion of a scheme is introduced. The sections up to varieties are from [39]. The section on varieties, especially notion of k -scheme and k -variety is from [16]. Group scheme, group variety and homogeneous space is from [39].

3.1. SCHEMES

3.1.1. Spec of a Ring, Zariski Topology

Definition 69 Let A be a commutative ring, and denote by $\text{Spec}A$ the set of prime ideals of A .

For any ideal $\mathfrak{a}$ of A denote by $V(\mathfrak{a})$ all prime ideals that contain the ideal $\mathfrak{a}$

$$V(\mathfrak{a}) = \{\mathfrak{p} : \text{prime ideal of } A \mid \mathfrak{a} \subseteq \mathfrak{p}\}$$

Note that if $\mathfrak{a}_1 \subset \mathfrak{a}_2$ then $V(\mathfrak{a}_2) \subset V(\mathfrak{a}_1)$

Lemma 33 $\text{Spec}A$ is a topological space with the closed sets given by $V(\mathfrak{a})$ where $\mathfrak{a}$ are ideals (or even just subsets) of A . This means that

- (1) $\cap_{i \in I} V(\mathfrak{a}_i)$ is a closed set for any collection $\{\mathfrak{a}_i \mid i \in I\}$ of ideals or subsets of A .
- (2) For any finite collection $\mathfrak{a}_i$ ($i = 1, \dots, n$) of ideals or subsets of A , $\cup_{i=1}^n V(\mathfrak{a}_i)$ is a closed set.
- (3) $\emptyset$ and $\text{Spec}A$ are closed sets.

Remark: The topology on $\text{Spec}A$ is called the *Zariski topology*.

Note that if S is a subset of A and $\mathfrak{S}$ is the ideal generated by S , then $V(S) = V(\mathfrak{S})$.

$$V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) = V(\mathfrak{a}_1 \cdot \mathfrak{a}_2)$$

Note that if $\mathfrak{a}_i \subset \mathfrak{p}$ for $i = 1, 2$ then $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \subset \mathfrak{a}_i \subset \mathfrak{p}$

On the other hand, if $\mathfrak{p} \supset \mathfrak{a}_1 \cdot \mathfrak{a}_2$ and $\mathfrak{p} \notin V(\mathfrak{a}_1)$ i.e. $\mathfrak{p} \not\supset \mathfrak{a}_1$ then there exists $r \in \mathfrak{a}_1 - \mathfrak{p}$. For any $s \in \mathfrak{a}_2$, $rs \in \mathfrak{a}_1 \cdot \mathfrak{a}_2 \subset \mathfrak{p}$. Since $\mathfrak{p}$ is prime and $r \notin \mathfrak{p}$, $s \in \mathfrak{p}$ hence $\mathfrak{a}_2 \subset \mathfrak{p}$, or $\mathfrak{p} \in V(\mathfrak{a}_2)$.

Let $\mathfrak{a}_i$ be a collection of ideals and let $\sum_i \mathfrak{a}_i$ denote the ideal formed by their sum. Then we have

$$\bigcap_i V(\mathfrak{a}_i) = V\left(\sum_i \mathfrak{a}_i\right)$$

It is clear that if $\mathfrak{p} \supset \mathfrak{a}_i$ for all i then $\mathfrak{p} \supset \sum_i \mathfrak{a}_i$ from the definition of an ideal. On the other hand if $\mathfrak{p} \supset \sum_i \mathfrak{a}_i$ then $\mathfrak{p} \supset \mathfrak{a}_i$ for all i since $\sum_i \mathfrak{a}_i \supset \mathfrak{a}_i$, sum of ideals contains all its components.

Note that here by sum of ideals, what is meant is all finite sums performed in the ring, i.e.

$$\sum_i \mathfrak{a}_i = \{r_1 + \dots + r_k \mid r_j \in \mathfrak{a}_i \text{ for some } i\}$$

By product of two ideals is meant

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 = \left\{ \sum_{i=1}^k r_i s_i \mid r_i \in \mathfrak{a}_1, s_i \in \mathfrak{a}_2, k \in \mathbb{N} \right\}$$

Now note that $V((0)) = \text{Spec} A$ and $V(A) = \emptyset$

3.1.2. Remark on Products

If we have a countable collection of ideals $\mathfrak{a}_i$, then the sequence

$$\mathfrak{a}_1 \supset \mathfrak{a}_1 \cdot \mathfrak{a}_2 \supset \mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdot \mathfrak{a}_3 \supset \dots$$

is an infinite sequence. If the ring is Artinian, this sequence is eventually stabilizes. One could consider all possible such sequences formed from countable collection, and inquire if under some assumptions it might be possible to define the product of an infinite collection of ideals. But this is not done in general.

What if we were to define the product of an arbitrary collection as finite sums of finite products with each term in the product coming from some element in the collection? Obviously sum of two such objects is still in the collection. On the other hand, if we multiply

such an element by an element from the ring, then the product is also in the collection. Hence this is an ideal.

Alternatively starting with an arbitrary collection of ideals, one can form the sum of these ideals, the sum of two-fold products of these ideals, the sum of three-fold products of these ideals and so forth, obtaining a countable sequence of ideals that is decreasing. One could then consider the intersection of these ideals, i.e.

$$\sum_i \mathfrak{a}_i \supset \sum_{i,j} \mathfrak{a}_i \cdot \mathfrak{a}_j \supset \sum_{i,j,k} \mathfrak{a}_i \cdot \mathfrak{a}_j \cdot \mathfrak{a}_k \supset \dots$$

Before continuing this, note that if $\mathfrak{a}_1 + \mathfrak{a}_2 = A$ then

$$V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2) = V(\mathfrak{a}_1 + \mathfrak{a}_2) = V(A) = \emptyset$$

Moreover,

$$V(\text{Rad}(\mathfrak{a})) = V(\mathfrak{a})$$

In order to see this, note that if $\mathfrak{p}$ is a prime ideal containing the radical of $\mathfrak{a}$ then since $\mathfrak{a}$ is contained in the radical, $\mathfrak{p}$ contains $\mathfrak{a}$ as well. On the other hand, if $\mathfrak{p}$ is an ideal containing $\mathfrak{a}$, and $s \in \text{Rad}(\mathfrak{a})$ i.e. $s^m \in \mathfrak{a}$ for some m , then $s^m \in \mathfrak{p}$ hence $s \in \mathfrak{p}$.

3.1.3. Elements of the Ring as Functions on Spec of the Ring

Definition 70 For every $\mathfrak{p} \in \text{Spec} A$ define the residue field $\kappa(\mathfrak{p})$ as the ring of fractions of $A/\mathfrak{p}$.

Definition 71 For every $f \in A$ one defines a function $\text{Spec} A \rightarrow \coprod_{\mathfrak{p} \in \text{Spec} A} \kappa(\mathfrak{p})$ given by $f(\mathfrak{p}) = [f] \in \kappa(\mathfrak{p})$ where $[f]$ denotes the class of f in the residue field $\kappa(\mathfrak{p})$.

Note that if $f \in \cap_{\mathfrak{p} \in \text{Spec} A} \mathfrak{p}$, then f defines the zero function. More generally, f assumes the value zero at all the prime ideals that it belongs to.

3.1.4. Polynomials over an Algebraically Closed Field

If k is an algebraically closed field, then $k[x]$ is a principal ideal domain, whose prime ideals are $(x - a)$ where $a \in k$. Hence $\text{Spec} k[x] \cong k \cup \{(0)\}$ where $(0) \subset (x - a)$ for all $a \in k$.

On the other hand the following known as Hilbert's Nullstellensatz-Weak form, specifies

maximal ideals of $k[x_1, \dots, x_n]$ for k algebraically closed:

Theorem 4 (Hilbert's Nullstellensatz-Weak Form) *For k an algebraically closed field, the maximal ideals of the polynomial ring $k[x_1, \dots, x_n]$ are of the form $\mathfrak{M} = (x_1 - a_1, \dots, x_n - a_n)$ for some $a_1, \dots, a_n \in k$. In other words there is a one-to-one correspondence between maximal ideals of $k[x_1, \dots, x_n]$ and points on $\mathbb{A}^n(k)$.*

3.1.5. Sheaves

The open subsets of a topological space X form a category denoted by $\text{Top}(X)$ whose morphisms are inclusion of one open set in another, when one open set is contained in another. In other words, for U, V being open sets in the topological space X , $\text{Hom}(U, V)$ consists of the single element, the inclusion $\iota_{U,V} : U \hookrightarrow V$ whenever $U \subseteq V$ and is empty otherwise.

Definition 72 *A presheaf $\mathcal{F}$ is a contravariant functor from the category of open sets of a topological space to a category $\mathcal{C}$ (usually abelian groups, rings, R -modules for a fixed ring R), that maps the initial object of the topology (i.e. the empty set) to the terminal object of $\mathcal{C}$ (i.e. abelian group with a single element or the zero ring). Explicitly this means, for a topological space X , If $\mathcal{F} : \text{Top}(X) \rightarrow \mathcal{C}$ denotes the functor defining the presheaf, then*

- *For each open set U of X , $\mathcal{F}(U)$ is an object of $\mathcal{C}$ (i.e. an abelian group or a ring or an R -module)*
- *The empty set is mapped to the zero object (of abelian groups, rings, or R -modules), i.e. $\mathcal{F}(\emptyset) = 0$*
- *Whenever U, V are open sets of X with $U \subseteq V$ then there exist morphisms $r_{V,U} : \mathcal{F}(V) \rightarrow \mathcal{F}(U)$ in $\mathcal{C}$ (i.e. homomorphism of abelian groups or rings or R -modules), called restriction morphisms.*
- *Restriction morphism corresponding to identity of an open set is identity, i.e. for U an open set of X , $\mathcal{F}(\text{id}_U) = r_{U,U} = \text{id}_{\mathcal{F}(U)}$.*
- *Restriction morphisms are transitive, i.e. if $U \subseteq V \subseteq W$ are open subsets of X then*

$$r_{W,U} = r_{V,U} \circ r_{W,V}$$

Given a presheaf $\mathcal{F} : \text{Top}(X) \rightarrow \mathcal{C}$, a section of the presheaf $\mathcal{F}$ over an open subset U of X is an element of $\mathcal{F}(U)$. The (set of) sections of a presheaf are also denoted by $\Gamma(U, \mathcal{F})$, instead of $\mathcal{F}(U)$.

A sheaf is a presheaf such that local conditions uniquely define a global element. To make the ideas precise consider the following. Let $\mathcal{F} = \mathcal{O}_X$, be a presheaf.

Now given two open sets U and V there are inclusion maps of $U \cap V$ into U and V . Under a presheaf, they correspond to restriction morphisms.

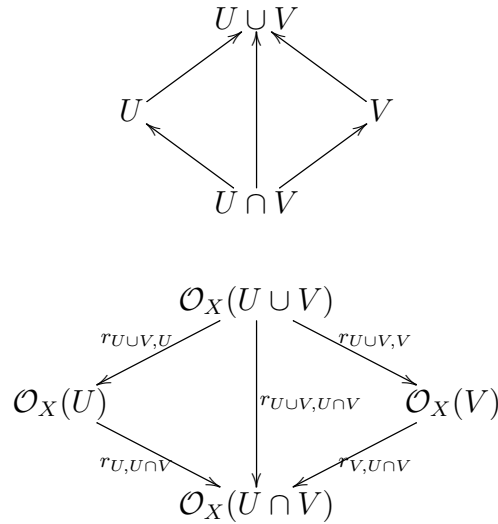
Now if one can find elements (local elements) $s_U \in \mathcal{O}_X(U)$ and $s_V \in \mathcal{O}_X(V)$ such that

$$r_{U, U \cap V}(s_U) = r_{V, U \cap V}(s_V)$$

(that are compatible) then there should exist an element $s \in \mathcal{O}_X(U \cup V)$ (more global element) such that $r_{U \cup V, U}(s) = s_U$ and $r_{U \cup V, V}(s) = s_V$ (that represents the local elements).

Of course the condition for two sets can be generalized to finitely many, and even arbitrarily many as it will be

Note that the above can be summarized in the diagrams



Now one can define a morphism

$$\mathcal{O}_X(U) \times \mathcal{O}_X(V) \rightarrow \mathcal{O}_X(U \cap V)$$

by

$$(s_U, s_V) \mapsto r_{U, U \cap V}(s_U) - r_{V, U \cap V}(s_V)$$

whenever subtraction is defined on objects of $\mathcal{C}$. Alternatively one can speak of the difference kernel of the two maps $r_{U, U \cap V}$ and $r_{V, U \cap V}$. Now the first condition for being a sheaf (instead of just a presheaf) is the requirement that the kernel of this map is the image of the map

$$\mathcal{O}_X(U \cup V) \rightarrow \mathcal{O}_X(U) \times \mathcal{O}_X(V)$$

defined via the restriction maps

$$s \mapsto (r_{U \cup V, U}(s), r_{U \cup V, V}(s))$$

i.e. that the sequence

$$\mathcal{O}_X(U \cup V) \rightarrow \mathcal{O}_X(U) \times \mathcal{O}_X(V) \rightarrow \mathcal{O}_X(U \cap V)$$

be an exact sequence.

We have one more requirement: the map $\mathcal{O}_X(U \cup V) \rightarrow \mathcal{O}_X(U) \times \mathcal{O}_X(V)$ should be injective. i.e. if for $s \in \mathcal{O}_X(U \cup V)$ $r_{U \cup V, U}(s) = r_{U \cup V, V}(s) = 0$ then $s = 0$.

Now if the sheaf is a sheaf of groups, then subtraction is replaced with multiplying by the inverse of the second element. In case of a ring, then one can still perform subtraction, but the resulting morphism will not be a ring homomorphism.

However the definition of being a sheaf is not for an arbitrary pair of open sets, but an arbitrary collection of open sets. In other words, the above conditions must be replaced by the exactness of the sequence

$$1 \rightarrow \mathcal{O}_X(\cup_i U_i) \rightarrow \prod_{i,j} \mathcal{O}_X(U_i) \times \mathcal{O}_X(U_j) \rightarrow \prod_{i,j} \mathcal{O}_X(U_i \cap U_j)$$

One could also inquire if the restriction maps are required to be surjective. This does not have to be the case, as in the example of rational functions with denominators having zeros outside an open set, do not have to lift to a larger domain.

Note for example analytic continuation of holomorphic functions in the complex plane. This

is carried out with the idea presented in the definition of sheaves. Also note that considering triple or more intersections probably won't create a new definition, but it could conceivably be written out.

Definition 73 A sheaf $\mathcal{F}$ on a topological space X (with values in category $\mathcal{C}$ which is the category of abelian groups or rings or R -modules) is a presheaf satisfying the following two conditions: For V_i a collection of open subsets of X and $V = \cup_i V_i$

- (i) For $s \in \mathcal{F}(V)$, $r_{V, V_i}(s) = \mathcal{F}(V_i \hookrightarrow V)(s) = 0$ for all i implies that $s = 0$. i.e.
- (ii) If there exist $s_i \in \mathcal{F}(V_i)$ such that for all pairs (i, j)

$$r_{V_i, V_i \cap V_j}(s_i) = r_{V_j, V_i \cap V_j}(s_j)$$

then there exists $s \in \mathcal{F}(V)$ such that $r_{V, V_i}(s) = s_i$ for all i

As discussed above, the first condition is equivalent to

$$\mathcal{F}(V) \longrightarrow \prod_i \mathcal{F}(V_i)$$

being injective. The second condition is equivalent to

$$\mathcal{F}(V) \longrightarrow \prod_i \mathcal{F}(V_i) \rightrightarrows \prod_{i,j} \mathcal{F}(V_i \cap V_j)$$

being exact, in the sense described before.

Definition 74 Stalk at a point p of a topological space X with a presheaf $\mathcal{O}_X$ of rings/groups is defined as

$$\mathcal{O}_p = \varinjlim_{p \in U} \mathcal{O}_X(U)$$

where the morphisms used defining the direct limit are the restriction morphisms of the presheaf, which are group or ring homomorphisms.

Elements of the stalk $\mathcal{F}_P$ for $P \in X$ are represented by pairs $\langle U, s \rangle$ where U is an open set of X and $s \in \mathcal{F}(U)$, where $\langle U, s \rangle = \langle V, t \rangle$ as elements of $\mathcal{F}_P$ if P has a neighborhood $W \subseteq U \cap V$ such that $r_{U, W}(s) = r_{V, W}(t)$. Elements of the stalk $\mathcal{F}_P$ are also referred as germs of sections of $\mathcal{F}$ at P .

Definition 75 A morphism of (pre)sheaves $\mathcal{F}, \mathcal{G} : \text{Top}(X) \rightarrow \mathcal{C}$ on a topological space X is a natural transformation from $\mathcal{F}$ to $\mathcal{G}$. This means for each open subset U of X there is a morphism in $\mathcal{C}$ $\phi(U) : \mathcal{F}(U) \rightarrow \mathcal{G}(U)$ such that whenever $U \subseteq V$, one has the commutative diagram:

$$\begin{array}{ccc} \mathcal{F}(V) & \xrightarrow{\phi(V)} & \mathcal{G}(V) \\ r_{V,U}^{\mathcal{F}} \downarrow & & \downarrow r_{V,U}^{\mathcal{G}} \\ \mathcal{F}(U) & \xrightarrow{\phi(U)} & \mathcal{G}(U) \end{array}$$

Proposition 1 • A morphism $\phi : \mathcal{F} \rightarrow \mathcal{G}$ of presheaves on a topological space X induces a morphism $\phi_P : \mathcal{F}_P \rightarrow \mathcal{G}_P$ on the stalks for each point $P \in X$.

- If ϕ is a morphism of sheaves, then ϕ is an isomorphism if and only if ϕ_P is an isomorphism for every $P \in X$.

Remark: For each open set V of P in X , $\phi(V) : \mathcal{F}(V) \rightarrow \mathcal{G}(V)$ is a group or ring homomorphism, and is compatible with restriction morphisms of $\mathcal{F}$ and $\mathcal{G}$ (since ϕ is a natural transformation from $\mathcal{F}$ to $\mathcal{G}$). Therefore there exists a morphism

$$\mathcal{F}_P = \varinjlim_{P \in V} \mathcal{F}(V) \rightarrow \varinjlim_{P \in V} \mathcal{G}(V) = \mathcal{G}_P$$

It is possible to construct a sheaf out of a presheaf, and a morphism of presheaves from the presheaf to the constructed sheaf, such that any morphism of presheaves from the presheaf to any other sheaf factors through this morphism. The constructed sheaf is also referred as sheafification of the presheaf, adjoint to the forgetful functor or inclusion functor of sheaves inside presheaves.

The construction is done via the stalks. The elements of the sheafification are functions that map each open set to the union of the stalks at the points in the open set, together with two additional conditions: (i) each point must be mapped to an element of the stalk at that point (ii) each point has a neighborhood within which the value of the function considered at each of those points must be given by the equivalence class defined by an element of the image of the neighborhood under the presheaf in the stalk at that point. This is written symbolically below. Note that these conditions mean that in the sheafification we are considering functions with values in the stalks at that point that are locally given by

elements of the presheaf.

Proposition 2 *Given a presheaf $\mathcal{F}$, there is a sheaf $\mathcal{F}^+$ and a morphism of presheaves $\theta : \mathcal{F} \rightarrow \mathcal{F}^+$ such that any morphism ϕ of presheaves from $\mathcal{F}$ to any sheaf $\mathcal{G}$ factors through θ , i.e. there is a morphism of sheaves $\psi : \mathcal{F}^+ \rightarrow \mathcal{G}$ such that $\phi = \psi \circ \theta$. The pair $(\mathcal{F}^+, \theta)$ is unique up to isomorphism.*

The elements of $\mathcal{F}^+(U)$ are given by functions $s : U \rightarrow \cup_{P \in U} \mathcal{F}_P$ such that

(i) For each $P \in U$ $s(P) \in \mathcal{F}_P$

(ii) For each $P \in U$ there is a neighborhood V of P inside U , and $t \in \mathcal{F}(V)$ such that for all $Q \in V$, the germ t_Q of t at Q (element of $\mathcal{F}_Q$ defined by the pair (V, t)) is equal to $s(Q)$.

$\mathcal{F}^+$ is called the sheaf associated to the presheaf $\mathcal{F}$.

Note that if s is a function satisfying the properties above on an open set U , and U' is an open subset of U then restriction of this function on U' satisfies the same properties for U' , by invoking the restriction morphism of the presheaf from V to $V \cap U'$ for second condition. Note that the germ obtained is the same, i.e. $t_Q = (r_{V, V \cap U'}(t))_Q$ for $t \in \mathcal{F}(V)$ and $Q \in U' \cap V$.

3.1.6. Sheaf on Spec of a Ring

Definition 76 *For a prime ideal $\mathfrak{p}$ of A denote by $A_{\mathfrak{p}}$ the localization of A at the prime ideal $\mathfrak{p}$, i.e. $A_{\mathfrak{p}} = (A - \mathfrak{p})^{-1}A$ is the ring obtained by forming fractions with all elements of A outside the prime ideal $\mathfrak{p}$.*

For an element $a \in A$ one defines the localization at a as $A_a = A[a^{-1}] = (a)^{-1}A$.

Note also that one can form the presheaf on $\text{Spec} A$ by defining a presheaf as $\mathcal{O}^{\text{pre}}$ by $\mathcal{O}^{\text{pre}}(U) = D(U)^{-1}A$ where $D(U) = A - \cup_{\mathfrak{q} \in U} \mathfrak{q} = \cap_{\mathfrak{q} \in U} A - \mathfrak{q}$. Note that $A - \mathfrak{q} \supset D(U)$ for each $\mathfrak{q} \in U$, so that one can see $A_{\mathfrak{q}} \supset D(U)^{-1}A$. If $V \subset U$, then $D(V) \supset D(U)$, and $D(V)^{-1}A \supset D(U)^{-1}A$, and there is the natural inclusion of rings from $D(U)^{-1}A$ into $D(V)^{-1}A$, which serves as the restriction homomorphism. (Note if one were dealing with polynomial functions as a ring, then this would correspond to restricting a rational function with zeros outside an open set to the rational function on a smaller open set). On

the other hand, the stalk of $\mathcal{O}^{\text{pre}}(U)$ at a point $\mathfrak{p}$ is the direct limit $\varinjlim_{U: \mathfrak{p} \in U} D(U)^{-1}A \cong A_{\mathfrak{p}}$, since in the direct limit one identifies points of $D(U)^{-1}A$ with those of $D(V)^{-1}A$ whenever $\mathfrak{p} \in V \subset U$, hence the quotient of $\cup_{\mathfrak{p} \in U} D(U)^{-1}A$ under this identification yields nothing but $A_{\mathfrak{p}}$. As a consequence of this discussion, the sheafification of this presheaf on $\text{Spec } A$ gives the following sheaf on $\text{Spec } A$:

Definition 77 For an open set $U \subset \text{Spec } A$ define

$$\mathcal{O}(U) = \{s : U \rightarrow \coprod_{\mathfrak{p} \in U} A_{\mathfrak{p}} \mid \forall \mathfrak{p} \in U \exists V \text{ neighborhood of } \mathfrak{p}, V \subseteq U \text{ such that}$$

$$\exists a \in A, f \in A - \cup_{\mathfrak{q} \in V} \mathfrak{q} \text{ with } s(\mathfrak{q}) = \frac{a}{f} \in A_{\mathfrak{q}} \forall \mathfrak{q} \in V\}$$

For $U \subseteq V$, define $r_{V,U} : \mathcal{O}(V) \rightarrow \mathcal{O}(U)$ by $r_{V,U}(s) = s \circ \iota_{U,V}$ where $\iota_{U,V} : U \rightarrow V$ is inclusion.

Clearly the sum and product of two such functions satisfies the same condition, hence $\mathcal{O}(U)$ is a ring. The constant function 1 is an identity of this ring.

Lemma 34 $\mathcal{O}$ defined above is a sheaf on $\text{Spec } A$.

Properties of this sheaf:

For $a \in A$ denote by $D(a) = \text{Spec } A - V((a))$. These are called basic open sets.

Note $\mathfrak{p} \in D(a)$ if and only if $\mathfrak{p} \not\supseteq (a)$ i.e. the set $(a) - \mathfrak{p}$ is nonempty.

- The stalk $\mathcal{O}_{\mathfrak{p}}$ is isomorphic to $A_{\mathfrak{p}}$
- For any $a \in A$ the ring $\mathcal{O}(D(a))$ is isomorphic to the localized ring A_a
- $\mathcal{O}(\text{Spec } A) \cong A$.

3.1.7. Scheme

3.1.7.1. Preliminary Definitions for a Scheme

Given a continuous map from one continuous space into another, a sheaf on the domain of the function induces a sheaf on the image by considering the sheaf (this is a sheaf) taking the preimage of each open set of the image under the continuous map. Note that a continuous map from a topological space X into a topological space Y can be said to induce a functor

from the category of topological space Y to the category of the topological space X . Each open subset V which is an object of the category $\text{top}Y$, is assigned by this functor $f^{-1}(V)$. Now a sheaf on Y is a contravariant functor from $\text{top}Y$ to $\mathbf{Ab}$ or $R - \mathbf{Mod}$ (R -modules for some ring R). Composition of the two functors (the one induced by f from $\text{top}Y$ to $\text{top}X$, which could be shown by f^{-1} , followed by the sheaf on X) gives a presheaf on Y . The remaining conditions for being a sheaf are also satisfied: if U is an open set of Y with $\{V_i \mid i \in I\}$ an open cover of U , then $f^{-1}(U)$ is an open set of X with $\{f^{-1}(V_i) \mid i \in I\}$ is an open cover of $f^{-1}(U)$. If s is a section of $\mathcal{F}(f^{-1}(U))$ of the presheaf obtained by taking the composition of a sheaf $\mathcal{F}$ on X with f^{-1} over an open set U of Y , and the restriction of s to each member V_i of the open cover is zero, then $\mathcal{F}$ being a sheaf implies $s = 0$. Note here that s can be viewed both as an element of the $\Gamma(U, \mathcal{F} \circ f^{-1})$ sections of the presheaf $\mathcal{F} \circ f^{-1}$ over U and $\Gamma(f^{-1}(U), \mathcal{F})$ sections of the sheaf $\mathcal{F}$ over $f^{-1}(U)$. (Note restriction morphisms of the presheaf on X and sheaf on Y coincide). The same reasoning shows that $\mathcal{F} \circ f^{-1}$ satisfies the second condition, i.e. locally defined and locally compatible sections determine a global section. f^{-1} as a functor from $\text{Top}Y$ to $\text{Top}X$ behaves nicely that its composition with a sheaf on Y determines a sheaf on X .

Definition 78 If $f : X \rightarrow Y$ is a continuous map, and $\mathcal{F}$ is a sheaf on topological space X then the direct image sheaf $f_*(\mathcal{F})$ on Y is defined by

$$f_*(\mathcal{F})(V) = \mathcal{F}(f^{-1}V)$$

for any open set V of Y .

However going in the other direction is not as direct. Image of an open set under a continuous map need not be open (nor contain a nonempty open set). Instead one considers the open sets containing the image of an open set under the function. The restriction morphisms of the sheaf on the image set (codomain) allows us to take the injective (direct) limit. In this way one obtains a presheaf on the domain from a sheaf on the codomain. That this is a presheaf can either be argued directly from the definition. Alternatively one can consider the set

$$\mathcal{S}_f = \{s : \text{top}X \rightarrow \text{top}Y \mid s(U) \supset f(U), \text{ for } U_1 \supset U_2, s(U_1) \supset s(U_2)\}$$

where $\text{top}X$ denotes here the set of open subsets of a topological space X and define sheaves corresponding to each element of this by setting $\mathcal{G}_s(U) = \mathcal{F}(s(U))$ where $\mathcal{F}$ is a sheaf on Y . After this one can take the direct limit of sheaves over $s \in \mathcal{S}_f$ ordered by $s_1 \leq s_2$ if $s_1(U) \subset s_2(U)$ for all $U \in \text{top}X$, obtaining a presheaf on X . Now one can sheafify this presheaf.

Definition 79 *If $f : X \rightarrow Y$ is continuous and $\mathcal{G}$ is a sheaf on Y then the inverse image sheaf $f^{-1}(\mathcal{G})$ on X is defined as the sheaf associated to the presheaf $U \mapsto \varinjlim_{V \supset f(U)} \mathcal{G}(V)$*

Definition 80 *A ring is a local ring if it has a unique maximal ideal. A ring is a local ring if and only if nonunits form an ideal (which is the unique maximal ideal).*

A homomorphism $\phi : A \rightarrow B$ of local rings A, B with maximal ideals $\mathfrak{m}_A$ and $\mathfrak{m}_B$ is a local homomorphism if $\phi^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$.

Note that the localization of a ring at a prime ideal is a local ring, the ring of p -adic integers is also a local ring. The definition of a local ring is reviewed in order to define a locally ringed space which is used in defining an affine scheme.

Definition 81 *A ringed space $(X, \mathcal{O}_X)$ is a topological space with a sheaf of rings $\mathcal{O}_X$. A ringed space is a locally ringed space if the stalks $\mathcal{O}_{X,P}$ are local rings for each $P \in X$.*

A morphism of ringed spaces $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ consists of a pair $(f, f^\#)$ where $f : X \rightarrow Y$ is a continuous map, and $f^\# : \mathcal{O}_Y \rightarrow f_*(\mathcal{O}_X) = \mathcal{O}_X \circ f^{-1}$ is a map (morphism) between sheaves of rings on Y .

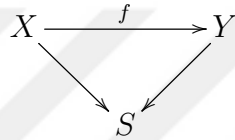
A morphism of locally ringed spaces $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ is a morphism $(f, f^\#)$ of ringed spaces such that for each point $P \in X$, the induced morphism of local rings $f_P^\# : \mathcal{O}_{Y,f(P)} \rightarrow \mathcal{O}_{X,P}$ is a local homomorphism of local rings.

3.1.7.2. Definition of an Affine Scheme and Scheme

A scheme is locally an affine scheme. In more detail,

Definition 82 • *An affine scheme is a locally ringed space $(X, \mathcal{O}_X)$ (i.e. a topological space with a sheaf of rings on it, such that the stalks are local rings), which is isomorphic as a locally ringed space to the spectrum of some ring. $\mathcal{O}_X$ is referred as the structure sheaf.*

- A scheme is a locally ringed space in which every point has an open neighborhood U such that $(U, \mathcal{O}_X|_U)$ is an affine scheme. ($\mathcal{O}_X|_U$ refers to the restriction of the sheaf $\mathcal{O}_X$ to subsets of U .)
- Morphism of schemes is a morphism between them as locally ringed spaces.
- A scheme over a fixed scheme S is a scheme X together with a morphism $X \rightarrow S$
- A morphism between schemes X and Y over a fixed scheme S is a morphism f of schemes between X and Y that is compatible with the morphisms $X \rightarrow S$ and $Y \rightarrow S$ i.e. those that form a commutative diagram



3.1.8. Smoothness

Smoothness is intuitively lack of sharp corners or edges. Smoothness fails if the tangent space at a point has dimension less than the dimension of the space. For schemes which are built locally out of spectrum of rings the notion of dimension is defined by Krull dimension. The tangent space is defined as dual of the quotient of the maximal ideal of the stalk by the square of the maximal ideal. The dimension of the tangent space is the dimension of this quotient as a vector space over the residue field.

Note that for an affine variety over a field its dimension is defined as the transcendence degree of its function field [26] p 681. Nonsingularity of a point of an affine variety is defined by a condition similar to the condition given for schemes below [26] p 725, where dimension of the stalk is replaced with dimension of the variety.

- Definition 83**
- Height of a prime ideal of a ring is the supremum of all integers n such that there exists a chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_n = \mathfrak{p}$ of distinct prime ideals.
 - Dimension of a ring is the supremum of heights of all prime ideals, this is also called Krull dimension.

Definition 84 A local ring A with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$ is a regular local ring if $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim A$

Definition 85 • A scheme is nonsingular at a point if the local ring defined by the stalk at that point $\mathcal{O}_P$ is a regular local ring.

- A scheme is smooth if all of its points are nonsingular.

3.1.9. Projective Schemes

Projective space over a field k of dimension n could be defined as the set of lines through the origin in k^{n+1} , or one-dimensional subspaces of k^{n+1} . To translate this notion into scheme theory takes some work. When one considers how rational functions and polynomials can be made to sensibly define functions on projective space, one arrives at the notion of homogeneity of polynomials. A polynomial which is a sum of monomials of same total degree d is called a homogeneous polynomial of degree d . The ratio of two homogeneous polynomials of same total degree defines a function on projective space. Due to these facts on projective spaces, the definition of a projective scheme is defined as below.

Projective over an affine scheme $\text{Spec} A$:

Definition 86 Let S be a positively graded finitely generated A -algebra, having A as the degree zero part, $S = \bigoplus_{i \in \mathbb{N}} S_i$, with $S_0 = A$, such that $S_i S_j \subset S_{i+j}$. Such an algebra S will be called the coordinate ring of the projective scheme $\text{Proj} S$. Assume for simplicity that S is generated by degree one elements.

An element $s \in S$ is called a homogeneous element if $s \in S_i$ for some i .

A homogeneous ideal of S is an ideal I such that $I = \bigoplus_{i \in \mathbb{N}} S_i \cap I$, or one that is generated by homogeneous elements.

Irrelevant ideal: $S_+ = \bigoplus_{i \geq 1} S_i$

$\text{Proj} S$ is the set of homogeneous prime ideals that do not contain S_+ .

Closed sets are defined similarly, for homogeneous ideals I

$$V(I) = \{\mathfrak{p} \in \text{Proj} S \mid I \subset \mathfrak{p}\}$$

Sheaf on $\text{Proj} S$ is defined similarly: let $S_{(\mathfrak{p})} = T^{-1} S$ where T is the multiplicative system

consisting of all homogeneous elements of S which are not in $\mathfrak{p}$.

$$\mathcal{O}(U) = \{s : U \rightarrow \coprod_{\mathfrak{p} \in U} S_{(\mathfrak{p})} \mid \forall \mathfrak{p} \in U \exists V \text{ neighborhood of } \mathfrak{p}, V \subseteq U \text{ such that}$$

$$\exists a \in S, f \in S - \cup_{\mathfrak{q} \in V} \mathfrak{q} \text{ with } s(\mathfrak{q}) = \frac{a}{f} \in S_{(\mathfrak{q})} \forall \mathfrak{q} \in V\}$$

and a and f are homogeneous elements of same degree.

Properties

- The stalk $\mathcal{O}_{\mathfrak{p}}$ is isomorphic to the local ring $S_{(\mathfrak{p})}$
- For any homogeneous $f \in S_+$ let $D_+(f) = \{\mathfrak{p} \in \text{Proj} S \mid f \notin \mathfrak{p}\}$ Then this is open in $\text{Proj} S$ and these open sets cover $\text{Proj} S$ For each open set we have an isomorphism of locally ringed spaces

$$(D_+(f), \mathcal{O}|_{D_+(f)}) \cong \text{Spec} S_{(f)}$$

- $\text{Proj} S$ is a scheme.

3.2. PROPERTIES OF SCHEMES

A scheme is a topological space where the topology comes from an algebraic structure. In this section properties of schemes are introduced. Of these irreducibility is a topological property. Usually topological properties have algebraic counterparts. For example an affine algebraic set is irreducible if and only if its ideal (the ideal vanishing on the variety) is prime [26] p680, [39] p 4. Connectedness is another topological property. Other properties such as being reduced or being integral are algebraically defined properties.

Definition 87 *A topological space is irreducible if it can not be written as the union of two proper closed subsets.*

Definition 88 *If X is a topological space and Z an irreducible closed subset of X , a generic point for Z is a point ζ such that Z is the closure of the set $\{\zeta\}$. (If X is a scheme, every nonempty irreducible closed subset has a unique generic point.)*

Definition 89 • *A scheme is connected if its topological space is connected.*

- *A scheme is irreducible if its topological space is irreducible.*

- A scheme is reduced if for every open set U , the ring $\mathcal{O}_X(U)$ has no nilpotent elements. (This is equivalent to requiring that the local rings $\mathcal{O}_P$ have no nilpotent elements.)
- A scheme is integral if for every U , the ring $\mathcal{O}_X(U)$ is an integral domain. (A scheme is integral if and only if both reduced and irreducible.)

Definition 90 • Dimension of a scheme is its dimension as a topological space, i.e. the supremum over all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \dots \subset Z_n$ of distinct closed irreducible subsets of X .

- If Z is an irreducible closed subset of a scheme X its codimension $\text{codim}(Z, X)$ is the supremum over all integers n such that there exists a chain $Z = Z_0 \subset Z_1 \subset \dots \subset Z_n$ of distinct irreducible closed subsets of X . If Y is any closed subset of X then its codimension is defined by

$$\text{codim}(Y, X) = \inf \{ \text{codim}(Z, X) \mid Z \subseteq Y, Z \text{ is closed and irreducible} \}$$

- If $X = \text{Spec} A$ is an affine scheme, then dimension of X is the same as the Krull dimension of A

3.2.1. Properties of Morphisms of Schemes: Locally of Finite Type, of Finite Type, Finite Morphism

Definition 91 • A morphism $f : X \rightarrow Y$ of schemes is locally of finite type if there exists a covering of Y by open affine subsets $V_i = \text{Spec} B_i$ such that for each i $f^{-1}(V_i)$ can be covered by open affine subsets $U_{ij} = \text{Spec} A_{ij}$ where each A_{ij} is a finitely generated B_i algebra.

- The morphism f is of finite type if in addition $f^{-1}(V_i)$ can be covered by a finite number of the U_{ij} .
- A morphism is a finite morphism if there exists a covering of Y by open affine subsets $V_i = \text{Spec} B_i$ such that for each i $f^{-1}(V_i)$ is affine and equal to $\text{Spec} A_i$ where A_i is a B_i -algebra which is a finitely generated B_i -module.

Lemma 35 If X is an affine integral scheme of finite type over a field k (i.e. the morphism

$X \rightarrow \text{Spec} k$ is of finite type) and Y is an irreducible closed subset of X then

$$\dim Y + \text{codim}(Y, X) = \dim X$$

3.2.2. Algebraic Scheme, Closed Subscheme

Definition 92 An algebraic scheme over a field K is a scheme together with a morphism of finite type from the scheme to $\text{Spec} K$.

In particular a morphism of algebraic schemes is assumed to be compatible with the structure morphism to $\text{Spec} K$. If f maps an affine open subset U' of X into an affine open subset U of Y then f corresponds to a homomorphism $f^* : A(U) \rightarrow A(U')$ of K -algebras, where $A(U)$ here denotes the coordinate ring of the affine open set U .

Some sources may require an algebraic scheme to be separated as well.

Remark: The following is not the only definition and is not the full definition, but gives enough of an idea what a closed subscheme is.

Definition 93 A closed subscheme of a scheme is defined by an ideal sheaf in the structure sheaf of the scheme, which corresponds, for an affine open covering of the scheme, an ideal in each coordinate ring of the scheme.

A closed subscheme comes equipped with a closed embedding.

3.3. PRODUCT OF SCHEMES

Products were defined for categories. Products of schemes over a base scheme is a scheme with projections to the constituent schemes that form a commutative diagram when composed with the morphisms to the base scheme, and is universal among all schemes that satisfy this property, i.e. given any other scheme satisfying the same commutative diagram, there is a morphism (of schemes) from this scheme to the (fibred) product that fits into a commutative diagram.

Definition 94 If X and Y are schemes over Z , then $X \times_Z Y$ is the scheme that forms a commutative diagram

$$\begin{array}{ccc} X \times_Z Y & \longrightarrow & X \\ \downarrow & & \downarrow \\ Y & \longrightarrow & Z \end{array}$$

commutative diagram, there is a (unique) morphism of schemes from this scheme to $X \times_Z Y$

If no mention of base scheme is made, it is taken as $\text{Spec}\mathbb{Z}$. When one considers $X \times_Z Y$ as a scheme over Y , one says that $X \times_Z Y$ is obtained from X as a scheme over Z by base extension to $Y \rightarrow Z$.

For affine schemes $X = \text{Spec}R$ and $Y = \text{Spec}S$ over $Z = \text{Spec}T$ the (fibered) product is the scheme $\text{Spec}(R \otimes_T S)$.

3.4. VARIETY

The term variety has several definitions that are slightly different in different sources. The intuitive notion is the zero set of a polynomial in several (but finitely many) variables with coefficients coming from a field. When one considers the zero set in projective n -space of a set of homogeneous polynomials, one is led to the notion of a projective variety.

Considering the functions defined by polynomials or rational functions on the varieties, and the algebraic structure of such functions leads to a generalization called schemes. Then varieties are defined as schemes with additional properties.

The first criterion has to do with the property of the stalks at each of the points in the scheme. This is almost always required to be reduced, i.e. nilpotent-free. This eliminates the polynomial defining the variety from being the power of some other polynomial.

The second criterion is irreducibility, which is not always required. Requiring irreducibility eliminates nonprime polynomials, hence forces one to look at the individual components of the geometric object.

If a scheme is both reduced and irreducible then it is integral (and vice versa).

The third property is being separated, which requires the diagonal morphism to be a closed immersion.

The following definition appears in Hartshorne [39].

Definition 95 *An abstract variety is an integral separated scheme of finite type over an algebraically closed field.*

Another difference in terminology comes from the field defining the coefficients of the polynomials. It may be that we are interested only in the points of the variety that lie in a certain field that lies strictly inside the algebraic closure.

Yet another difference comes from whether one is looking at the spectrum of prime ideals, or the spectrum of maximal ideals in the scheme.

In light of the last two considerations Borel in Linear Algebraic Groups gives the following definitions:

Definition 96 A k –algebra A is said to be affine, if it is finitely generated as a k –algebra. Such an A is a Noetherian ring.

Definition 97 Maximal spectrum of a finitely generated k –algebra A (where k is an algebraically closed field), is the set of maximal ideals in $\text{Spec} A$ is denoted by $\text{mSpec}(A)$ or $\text{Spec}_k(A)$. It is called the affine k –scheme.

Its sheaf is the sheaf associated to the presheaf

$$U \mapsto A[S(U)^{-1}]$$

where $S(U) = \{f \in A \mid f(p) \neq 0 \forall p \in U\}$ and $f(x)$ is the class of $f \in A$ in $A/x \cong k$ for $x \in \text{mSpec}(A) = \text{Spec}_k(A)$.

Stalk of this sheaf at $x \in X$ is the local ring A_x .

This sheaf is denoted by $\tilde{A}$.

For k algebraically closed field the following are defined.

- k –space: a topologically ringed space where the sheaf is a sheaf of k –algebras, and the part of their morphisms being local k –algebra homomorphisms
- k –scheme: a k –space that has a finite cover by affine k –schemes
- prevariety: reduced k –scheme
- algebraic variety: separated prevariety

and For K algebraically closed field and k a subfield of K :

- k –structure on a K –vector space V is a submodule V_k of V such that $V \cong V_k \otimes_k K$.
- k –structure on a K –scheme
- k –variety

The last two are defined below:

Definition 98 A k -structure on a K -scheme $(X, \mathcal{O}_X)$ consists of

- (1) A k -topology $k\text{-top}(X) \subset \text{top}(X)$
- (2) A k -structure on $\mathcal{O}_X(U)$ for each k -open U such that restriction homomorphisms are defined over k .

Remark

- Condition (2) says that the restriction of $\mathcal{O}_X$ to $k\text{-top}(X)$ is a sheaf of K -algebras with k -structures.
- It is further required that on k -open affine subschemes, the induced k -structure be of the following type:
 - A k -structure on an affine K -scheme $X = \text{spec}_K(A)$ is one defined by k -structure A_k on A as follows:

A set is k -closed if it is of the form $\text{supp}(A/J)$ for some ideal J defined over k .

Note $\text{supp}(M) = \{P \in A \mid M_P \neq 0\}$ where M_P is localization of M at P .

Definition 99 A morphism $\alpha : X \rightarrow Y$ of K -schemes with k -structures is defined over k or a k -morphism if

- (a) α is continuous relative to the k -topologies
- (b) If $U \subset Y$ and $V \subset X$ are k -open such that $\alpha(V) \subset U$ then $\alpha_V^U : \mathcal{O}_Y(U) \rightarrow \mathcal{O}_X(V)$ is defined over k . (alternatively $\alpha^\sharp$ is defined over k .)

Definition 100 A variety V with a k -structure will be called a k -variety.

3.4.1. Closed Subschemes

Another notion that plays a role later is the notion of a closed subscheme.

Definition 101 A closed immersion is a morphism $f : Y \rightarrow X$ of schemes such that f induces a homeomorphism of the space of Y onto a closed subset of the space of X and the induced map $f^\sharp : \mathcal{O}_X \rightarrow f_*\mathcal{O}_Y$ of sheaves on X is surjective.

A closed subscheme of a scheme X is an equivalence class of closed immersions where two closed immersions $f : Y \rightarrow X$ and $f' : Y' \rightarrow X$ are said to be equivalent if there is an isomorphism $i : Y \rightarrow Y'$ such that $f = f' \circ i$.

Definition 102 Let Y be a closed subscheme of a scheme, and $i : Y \rightarrow X$ be the inclusion morphism. The ideal sheaf of Y , denoted $\mathfrak{I}_Y$ is the kernel of the morphism $i^\sharp : \mathcal{O}_X \rightarrow i_*\mathcal{O}_Y$.

Proposition 3 Let X be a scheme. For any closed subscheme Y of X , the corresponding ideal sheaf $\mathfrak{I}_Y$ is a quasi-coherent sheaf of ideals on X . If X is Noetherian, it is coherent. Conversely any quasi-coherent sheaf of ideals on X is the ideal sheaf of a uniquely determined closed subscheme of X .

3.4.2. Sheaf of Modules, Quasi-coherent Sheaf

Definition 103 Let $(X, \mathcal{O}_X)$ be a ringed space. A sheaf of $\mathcal{O}_X$ -modules is a sheaf $\mathcal{F}$ on X such that for each open set $U \subseteq X$, the group $\mathcal{F}(U)$ is an $\mathcal{O}_X(U)$ -module and for each inclusion $V \subseteq U$ of open sets, the restriction morphism $\mathcal{F}(U) \rightarrow \mathcal{F}(V)$ is compatible with module structures via the ring homomorphism (restriction morphism) $\mathcal{O}_X(U) \rightarrow \mathcal{O}_X(V)$.

A morphism $\mathcal{F} \rightarrow \mathcal{G}$ of sheaves of $\mathcal{O}_X$ -modules is a morphism of sheaves such that the morphisms $\mathcal{F}(U) \rightarrow \mathcal{G}(U)$ is a homomorphism of $\mathcal{O}_X(U)$ -modules.

Definition 104 Let A be a ring, and M be an A -module. The sheaf associated to M on $\text{Spec}A$, denoted by $\tilde{M}$ is defined by

$$\tilde{M}(U) = \{s : U \rightarrow \coprod_{\mathfrak{p} \in U} M_{\mathfrak{p}} \mid \forall \mathfrak{p} \in U \ s(\mathfrak{p}) \in M_{\mathfrak{p}} \text{ and } s = m/f \ m \in M \ f \in A \text{ locally}\}$$

i.e. for each $\mathfrak{p} \in U$ there is a neighborhood V of $\mathfrak{p}$ in U and there are elements $m \in M$ and $f \in A$ such that for each $\mathfrak{q} \in V$, $f \notin \mathfrak{q}$ and $s(\mathfrak{q}) = m/f \in M_{\mathfrak{q}}$.

Note that $M_{\mathfrak{p}}$ denotes the localization of an A -module M at the prime $\mathfrak{p} \subseteq A$, i.e. $M_{\mathfrak{p}}$ is the $A_{\mathfrak{p}}$ -module $(A - \mathfrak{p})^{-1}M \cong A_{\mathfrak{p}} \otimes_A M$.

Definition 105 Let $(X, \mathcal{O}_X)$ be a scheme. A sheaf of $\mathcal{O}_X$ -modules $\mathcal{F}$ is quasi-coherent if X can be covered by open affine subsets $U_i = \text{Spec}A_i$ such that for each i there is an A_i -module M_i with $\mathcal{F}|_{U_i} \cong \tilde{M}_i$.

$\mathcal{F}$ is coherent if each M_i can be taken to be a finitely generated A_i -module.

Definition 106 A sheaf of ideals on X is a sheaf of modules $\mathfrak{I}$ which is a subsheaf of $\mathcal{O}_X$. i.e. $\mathfrak{I}(U)$ is an ideal in $\mathcal{O}_X(U)$.

Definition 107 • An $\mathcal{O}_X$ -module $\mathcal{F}$ is free if isomorphic to a direct sum of copies of $\mathcal{O}_X$.

- It is locally free if X can be covered by open sets U for which $\mathcal{F}|_U$ is a free $\mathcal{O}_X|_U$ -module.
- Rank of $\mathcal{F}$ on an open set U is the number of copies of the structure sheaf needed.
- A locally free sheaf of rank one is called an invertible sheaf.

3.4.3. Projective Variety

Definition 108 A projective variety is one isomorphic to a closed subvariety of a projective space $\mathbb{P}^n(k)$. A quasi-projective variety is an open subvariety of a projective variety. (Affine varieties are quasi-projective).

3.4.4. Separated Morphism

Definition 109 Let $f : X \rightarrow Y$ be a morphism of schemes. The diagonal morphism is the unique morphism $\Delta : X \rightarrow X \times_Y X$ whose composition with both projection maps $p_1, p_2 : X \times_Y X \rightarrow X$ is the identity map of $X \rightarrow X$. Morphism f is separated if the diagonal morphism Δ is a closed immersion. In that case, it is said that X is separated over Y . A scheme X is separated if it is separated over $\text{Spec}\mathbb{Z}$.

Proposition 4 If $f : Y \rightarrow Y$ is any morphism of affine schemes, then f is separated.

Corollary 2 An arbitrary morphism $f : X \rightarrow Y$ is separated if and only if the image of the diagonal morphism is a closed subset of $X \times_Y X$.

3.4.5. Proper Morphism, Complete Variety, Generic Point

Definition 110 A morphism $f : X \rightarrow Y$ (of schemes) is proper if it is separated, of finite type, and universally closed. Here we say that a morphism is closed if the image of any closed subset is closed. A morphism $f : X \rightarrow Y$ is universally closed if it is closed, and for any morphism $Y' \rightarrow Y$, the corresponding morphism $f' : X' \rightarrow Y'$ obtained by base extension is also closed.

Here $X' = X \times_Y Y'$ is said to be obtained from X by base extension.

Definition 111 *If an abstract variety is proper over k it is called complete.*

Definition 112 *A generic point of a variety/scheme is a point whose closure is the whole space.*

3.5. GROUP SCHEME, GROUP VARIETY, HOMOGENEOUS SPACE

Definition 113 *A scheme X with a morphism π to another scheme S is a group scheme over S if*

(identity) There is a section $e : S \rightarrow X$

(inverse) A morphism $\rho : X \rightarrow X$ over S called the inverse

(group operation) A morphism $\mu : X \times X \rightarrow X$ over S

such that

(1) - has inverses:

$$\mu \circ (\text{id} \times \rho) = e \circ \pi$$

(2) - satisfies associativity

$$\mu \circ (\mu \times \text{id}) = \mu \circ (\text{id} \times \mu)$$

Definition 114 *A group variety G over an algebraically closed field k is a variety G together with morphisms $\mu : G \times G \rightarrow G$ and $\rho : G \rightarrow G$ such that the set $G(k)$ of k -rational points of G (which is the set of all closed points of G) becomes a group under the operation induced by μ with inverses given by ρ .*

Definition 115 *A group variety G acts on a variety X if we have a morphism $\theta : G \times X \rightarrow X$ which induces a homomorphism $G(k) \rightarrow \text{Aut}(X)$ of groups.*

Definition 116 *A homogeneous space is a variety X together with a group variety G acting on it, such that the group $G(k)$ acts transitively on the set $X(k)$ of k -rational points of X .*

3.5.1. Affine Group Scheme

An affine group scheme G over some ring R is a scheme over spectrum of that ring, that comes with two maps $m : G \times G \rightarrow G$ and $i : G \rightarrow G$ such that G acquires a group structure with multiplication defined by m and inversion by i , and an element of G specified as identity.

An example is the general linear group $GL_n(R)$ of invertible $n \times n$ matrices with entries in R . Note that this is defined as $R[x_{11}, \dots, x_{nn}, t]/(\det(x_{ij})t - 1)$ (or rather the spectrum of that ring). Note that the actual matrices do appear as members of the spectrum as the maximal ideal $(x_{ij} - r_{ij}, t \det(x_{ij}) - 1)/(\det(x_{ij})t - 1) = (x_{ij} - r_{ij}, t \det(r_{ij}) - 1)/(t \det(x_{ij})t - 1)$ and the multiplication and inversion of matrices define a map on the spectrum, and although it won't be written explicitly also on the sheaves. Also we assume whatever is necessary on the ring.

4. TANNAKIAN CATEGORIES

The main source for this chapter is [78]. The actual definition of a Tannakian category is not given. This definition relies on nonabelian cohomology [31]. Instead a neutral Tannakian category is defined. Another source for definition of Tannakian categories is [22].

A tensor category is basically a category in which a product $\otimes$ on objects together with a way of identifying (i) $(A \otimes B) \otimes C$ and $A \otimes (B \otimes C)$ (associativity constraint), (ii) $A \otimes B$ and $B \otimes A$ (commutativity constraint), (iii) an identity object 1 and a way of identifying $1 \otimes A$ and $A \otimes 1$ with A (identity constraint). Note that the different forms do not have to be the same object, but need to be isomorphic objects.

The discussion on tensor categories deviates from [78] in the remark on associativity and commutativity constraint, basically outlining that the mixed associativity and commutativity constraints that would arise may need to be larger than a single condition.

A –modules for a commutative ring form as a basic example of a tensor category, with tensoring over A forming the tensor product.

Internal hom and reflexivity are defined for the purpose of defining a neutral Tannakian category.

For a commutative ring with unit A , and G an affine group A –scheme, the group G can be reconstructed as the group of tensor automorphisms of the forgetful functor from the linear representations of G as A –modules to A –modules. This result is proved in [78].

Of particular interest is what happens under a base change, when scalars are changed from one field to an extension for purposes of number theory. For this purpose descent theory was developed and there is a result analogous to the result above on the fiber functor that utilizes nonabelian cohomology in regards to Tannakian categories that is explored in the chapter3: Tannaka Duality in [78]. This is not treated in this thesis.

4.1. TENSOR CATEGORIES ($\otimes$ –CATEGORIES)

Definition 117 *For a category $\mathcal{C}$, a functor $\mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$ is called a tensor structure ($\otimes$ –structure, tensorial or $\otimes$ –law) over $\mathcal{C}$.*

A tensor category ($\otimes$ –category) is a category $\mathcal{C}$ equipped with a $\otimes$ –structure, that is

denoted by $\otimes_{\mathbf{C}}$ or simply $\otimes$ if this raises no confusion.

To each pair of objects X, Y of $\mathbf{C}$ the functor associates an object $X \otimes Y$ of $\mathbf{C}$ which depend functorially on (X, Y) .

To each pair of morphisms (f, g) the functor associates a morphism $f \otimes g : X_1 \otimes Y_1 \rightarrow X_2 \otimes Y_2$. (Here $f \in \text{Hom}_{\mathbf{C}}(X_1, X_2)$ and $g \in \text{Hom}_{\mathbf{C}}(Y_1, Y_2)$ so that $(f, g) \in \text{Hom}_{\mathbf{C} \times \mathbf{C}}((X_1, Y_1), (X_2, Y_2))$).

A functor from a tensor category $(\mathbf{C}, \otimes_{\mathbf{C}})$ to a tensor category $(\mathbf{D}, \otimes_{\mathbf{D}})$ is said to preserve tensor structure if

$$F(X \otimes_{\mathbf{C}} Y) = F(X) \otimes_{\mathbf{D}} F(Y)$$

and is called a tensorial functor.

Definition 118 Let A be a commutative ring with unit. Recall that an A -linear category is a category $\mathbf{C}$ such that for every pair of objects X, Y of $\mathbf{C}$, the set of morphisms (arrows) from X to Y $\text{Hom}_{\mathbf{C}}(X, Y)$ is equipped with an A -module structure, which depend functorially on (X, Y) .

Definition 119 Let A be a commutative ring with unit. An A -linear $\otimes$ - (tensor) structure over an A -linear category, is an A -bilinear functor $\mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$.

Definition 120 Let X be an object of a $\otimes$ -category (tensor category). One says that X is 0, 1, 2-regular on the left if the functor $Y \mapsto Y \otimes X$ from $\mathbf{C}$ to $\mathbf{C}$ is faithful, full and faithful, is an equivalence of categories. Similarly, the same is defined for tensoring on the right, and both.

(Recall a faithful functor is injective on morphisms, full functor is surjective on morphisms among objects that are in the image of the functor. Equivalence of categories is a pair of functors one from the domain category to the codomain category, the other going in the other direction, whose compositions are naturally isomorphic to the identity functors on each category.)

Definition 121 If $\mathbf{C}$ is a $\otimes$ -category with $\otimes$ -structure, the opposite $\otimes$ -structure if the opposite category $\mathbf{C}^o$ equipped with $\otimes$ -structure that is same on objects as the original

$\otimes$ –structure, and with arrows reversed.

Definition 122 The symmetric $\otimes$ –structure of $\mathbf{C}$ denoted by $\mathbf{C}^{\text{sym}}$ is the category $\mathbf{C}$ equipped with a $\otimes$ –structure formed by

$$\mathbf{C} \times \mathbf{C} \xrightarrow{\sigma} \mathbf{C} \times \mathbf{C} \xrightarrow{\otimes} \mathbf{C}$$

where σ is the canonical symmetry of $\mathbf{C}$ given by $\sigma(X, Y) = (Y, X)$.

Lemma 36

$$\begin{aligned} (\mathbf{C}^o)^o &= \mathbf{C} \\ (\mathbf{C}^o)^{\text{sym}} &= (\mathbf{C}^{\text{sym}})^o \\ (\mathbf{C}^{\text{sym}})^{\text{sym}} &= \mathbf{C} \end{aligned}$$

Lemma 37 Let $\mathbf{C}$ be a category in which products of objects exist. Choose a product $(X \times Y, p_X, p_Y)$. Define a $\otimes$ –structure (tensor structure) over $\mathbf{C}$ by defining the tensor product as the product in the category, and by defining morphisms via pairs (products) of morphisms. Then

- An object X of $\mathbf{C}$ is 0–regular if and only if it is a covering meaning that for each object Y of $\mathbf{C}$ the projection $p_Y \in \text{Hom}_{\mathbf{C}}(Y \times X, Y)$ is an epimorphism.
- An object X of $\mathbf{C}$ is 1–regular if and only if it is 2–regular or if it is a final (terminal) object of $\mathbf{C}$.

(Note terminal object, is an object in a category such that the morphism set to that object consists of a single element.)

Proof 1

$$\begin{array}{ccccc} Y_1 & \xrightarrow{\otimes X} & Y_1 \otimes X & \xrightarrow{p_{Y_1}} & Y_1 \\ f_i \downarrow & & \downarrow f_i \otimes \text{id}_X & & \downarrow f_i \\ Y_2 & \xrightarrow{\otimes X} & Y_2 \otimes X & \xrightarrow{p_{Y_2}} & Y_2 \end{array}$$

Assume that we choose two morphisms for $i = 1, 2$ in $f_1, f_2 \in \text{Hom}_{\mathbf{C}}(Y_1, Y_2)$. Suppose that

$f_1 \otimes \text{id}_X = f_2 \otimes \text{id}_X$. The commutativity of the diagram is evident from assumptions (The square diagram on the left follows from the definition of tensor structure, the square diagram on the right follows from definition of projection functor on products of categories). Then we have

$$f_i \circ p_{Y_1} = p_{Y_2} \circ (f_i \otimes \text{id}_X)$$

Then $f_1 \otimes \text{id}_X = f_2 \otimes \text{id}_X$ implies together with above that $f_1 \circ p_{Y_1} = f_2 \circ p_{Y_1} \cdot p_{Y_1}$ being epic would then imply that $f_1 = f_2$ proving that under the assumption of projections being epic, objects of $\mathbf{C}$ are 0-regular. Now suppose that objects of $\mathbf{C}$ are 0-regular, and $f_1 \circ p_{Y_1} = f_2 \circ p_{Y_1}$. Then from the commutativity of the diagram we have $p_{Y_2} \circ (f_1 \otimes \text{id}_X) = p_{Y_2} \circ (f_2 \otimes \text{id}_X)$. However at least in set projection is not monic, so I don't see how we can make further conclusions.

If an object is 2-regular, then from definition it follows that it is 1-regular. For the other direction, again maybe it is a difference of definitions, but for a 1-regular object, tensoring with it does not have to be surjective onto the objects of the category. Maybe the terminal object assumption could be utilized, by taking into accounts that morphisms into X consist of a single element and noting then forced commutativity of

$$\begin{array}{ccc} Y & \xrightarrow{\otimes X} & Y \otimes X \\ & \searrow & \swarrow \\ & X & \end{array}$$

There are more statements and examples following this in the text.

Modules over a commutative ring with unit, equipped with tensor product of modules.

Lemma 38 *For modules over a commutative ring with unit, such a module is 2-regular if and only if projective of rank 1.*

Proof 2

Lemma 39 *For a commutative ring with unit A , let $\bigvee L = \text{Hom}_A(L, A)$. If L is projective of rank 1 then one has the canonical isomorphisms*

$$\bigvee L \otimes L \cong A$$

$$L \otimes \bigvee L \cong A$$

By associativity of tensorial product of A -modules, the functor $X \mapsto X \otimes \bigvee L$ is a quasi-inverse of the functor $X \mapsto X \otimes L$.

Definition 123 A module M over a commutative ring A with unit is of finite type if it is finitely generated over that ring, in other words, if there exist $x_1, \dots, x_n \in M$ such that $A = \bigoplus_i Ax_i$.

Lemma 40 Suppose that L is 2-regular (in the category of A -modules where A is a commutative ring with unit). Then L is projective of finite type.

Proof 3 2-regularity means that the functor of tensoring with L is an equivalence of abelian categories. Effectually, L is the image of A under the equivalence provided by 2-regularity, and property of being projective and of finite type is preserved under equivalence. This is clear for being projective. For being of finite type note that an A -module M is of finite type if and only if for all inductive filter systems (N_α) within which the transition morphisms being monomorphisms, the canonical morphism

$$\varinjlim \text{Hom}(M, N_\alpha) \longrightarrow \text{Hom}(M, \varinjlim N_\alpha)$$

is an isomorphism.

Finally, L is of rank 1, because there exists an A -module L' and an isomorphism $L' \otimes L \cong A$ (the functor of tensoring with L is essentially surjective).

4.2. ASSOCIATIVITY CONSTRAINTS

Definition 124 Let $\mathbf{C}$ be a $\otimes$ -category (tensor category). An associativity constraint for $\mathbf{C}$ is a functorial isomorphism φ

$$\varphi_{X,Y,Z} : X \otimes (Y \otimes Z) \xrightarrow{\sim} (X \otimes Y) \otimes Z$$

such that for objects X, Y, Z, T one has the following commutative diagram (called the pentagon axiom):

$$\begin{array}{ccc}
 & (X \otimes Y) \otimes (Z \otimes T) & \\
 \varphi_{X,Y,Z \otimes T} \nearrow & & \searrow \varphi_{X \otimes Y,Z,T} \\
 X \otimes (Y \otimes (Z \otimes T)) & & ((X \otimes Y) \otimes Z) \otimes T \\
 \text{id}_X \otimes \varphi_{Y,Z,T} \downarrow & & \uparrow \varphi_{X,Y,Z} \otimes \text{id}_T \\
 X \otimes ((Y \otimes Z) \otimes T) & \xrightarrow{\varphi_{X,Y \otimes Z,T}} & (X \otimes (Y \otimes Z)) \otimes T
 \end{array}$$

The diagram is expressed by the equality:

$$\varphi_{X \otimes Y,Z,T} \circ \varphi_{X,Y,Z \otimes T} = (\varphi_{X,Y,Z} \otimes \text{id}_T) \circ \varphi_{X,Y \otimes Z,T} \circ (\text{id}_X \otimes \varphi_{Y,Z,T})$$

One calls a tensor category equipped with a constraint of associativity an associative tensor category.

Lemma 41 (Coherence) *Given an associativity constraint φ on a $\otimes$ -category $\mathbf{C}$ the following can be constructed:*

- (a) A law associated to each family $(X_i)_{i \in I}$ of objects of $\mathbf{C}$ indexed by a nonempty finite and totally ordered set $(I, <)$ an object of $\mathbf{C}$ depending functorially on X_i ($i \in I$) to be denoted by $\otimes_{I, <} X_i$, such that if (X) is such a reduced family consisting of a single object, then $\otimes(X) = X$
- (b) For two such families $(X_i)_{i \in I_1}$, and $(X_i)_{i \in I_2}$ a functorial isomorphism of X_i

$$\varphi : (\otimes_{I_1, <} X_i) \otimes (\otimes_{I_2, <} X_i) \rightarrow \otimes_{I, <} X_i,$$

where $I = I_1 \sqcup I_2$ equipped with order induced by the orders on I_1 and I_2 and $i_1 < i_2$ for all $i_1 \in I_1$ and $i_2 \in I_2$, such that for $X, Y, Z \in \text{ob} \mathbf{C}$ an isomorphism above composed with the two possible partitions of the ordered set where index of X is less than that of Y less than that of Z , and its inverse yields the associativity constraint $\varphi_{X,Y,Z}$.

Furthermore, such a law is unique in the sense that given two such laws satisfying above conditions, then there is a system of isomorphisms among all all such products (and finite families) compatible with associativity constraints, such that if the family is reduced to a

single element (object) then the isomorphism α is the identity morphism of that object.

Definition 125 Recall that group of automorphisms of a functor is the group of natural (self-)equivalences of that functor. It is denoted by $\text{Aut}(\cdot)$ where $\cdot$ is the name of the functor. If the functor preserves tensor structure (on the domain and codomain categories of the functor) then one denotes the group by $\text{Aut}^\otimes(\cdot)$.

Definition 126 Action of the group of automorphisms of tensor functor on associativity constrains:

The group $\text{Aut}(\otimes)$ of automorphisms of the functor $\otimes : \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$ acts on the left on the set $\text{Assoc}(\mathbf{C}, \otimes)$ of constraints of associativity for $\mathbf{C}$ in the following fashion: If $\varphi \in \text{Assoc}(\mathbf{C}, \otimes)$, and $c \in \text{Aut}(\mathbf{C})$ ${}^c\varphi$ is defined by the commutativity of the following diagram:

$$\begin{array}{ccc}
 X \otimes (Y \otimes Z) & \xrightarrow{\varphi_{X,Y,Z}} & (X \otimes Y) \otimes Z \\
 \text{id}_X \otimes c_{Y,Z} \downarrow & & \downarrow c_{X,Y} \otimes \text{id}_Z \\
 X \otimes (Y \otimes Z) & & (X \otimes Y) \otimes Z \\
 c_{X,Y \otimes Z} \downarrow & & \downarrow c_{X \otimes Y, Z} \\
 X \otimes (Y \otimes Z) & \xrightarrow{{}^c\varphi_{X,Y,Z}} & (X \otimes Y) \otimes Z
 \end{array}$$

One says that two elements of $\text{Assoc}(\mathbf{C}, \otimes)$ are cohomologous if they are in the same orbit for the action of $\text{Aut}(\otimes)$.

4.3. COMMUTATIVITY CONSTRAINTS

Definition 127 Let $\mathbf{C}$ be a $\otimes$ -category. A commutativity constraint of $\mathbf{C}$ is a functorial isomorphism ψ with

$$\psi_{X,Y} : X \otimes Y \xrightarrow{\sim} Y \otimes X$$

such that

$$\psi_{Y,X} \circ \psi_{X,Y} = \text{id}_{X \otimes Y}$$

A $\otimes$ -category equipped with commutativity constraint is called a commutative $\otimes$ -category.

Definition 128 *Action of the group of automorphisms of tensor functor on commutativity constraints: The group $\text{Aut}(\otimes)$ acts on the set $\text{Comm}(\mathbf{C}, \otimes)$ of constraints of commutativity for $\mathbf{C}$ in the following fashion: If $\psi \in \text{Comm}(\mathbf{C}, \otimes)$, and $c \in \text{Aut}(\mathbf{C})$ ${}^c\psi$ is defined by the commutativity of the following diagram:*

$$\begin{array}{ccc} X \otimes Y & \xrightarrow{\psi_{X,Y}} & Y \otimes X \\ c_{X,Y} \downarrow & & \downarrow c_{Y,X} \\ X \otimes Y & \xrightarrow{{}^c\psi_{X,Y}} & Y \otimes X \end{array}$$

Two constraints of commutativity for $\mathbf{C}$ are said to be cohomologous if they are in the same orbit under this action.

Definition 129 *For a $\otimes$ -category $\mathbf{C}$ equipped with a commutativity constraint ψ and an object X of $\mathbf{C}$ the automorphism $\psi_X = \psi_{X,X} : X \otimes X \xrightarrow{\sim} X \otimes X$ of order 2 is called canonical symmetry of $X \otimes X$.*

A commutativity constraint is said to be strict if canonical symmetries are identities. $\mathbf{C}$ is then called a strictly commutative $\otimes$ -category.

4.4. UNIT CONSTRAINTS

Definition 130 *A unit constraint for a $\otimes$ -category $\mathbf{C}$ (or more simply a unit for $\mathbf{C}$ is a triple $(1, l, r)$ where $1 \in \text{ob}(\mathbf{C})$, and l, r are functorial isomorphisms (natural equivalences)*

$$l_X : X \xrightarrow{\sim} 1 \otimes X$$

$$r_X : X \xrightarrow{\sim} X \otimes 1$$

verifying the condition

$$l_1 = r_1$$

Let r denote the isomorphism $l_1 = r_1$

One may remark that the object 1 is 2-regular.

If X is an object of $\mathbf{C}$ one sets the notation

$$\Gamma(X) = \text{Hom}(1, X)$$

Lemma 42

$$l_{1 \otimes X} = \text{id}_1 \otimes l_X$$

$$r_{X \otimes 1} = r_X \otimes \text{id}_1$$

$$l_{X \otimes 1} \circ r_X = (\text{id}_1 \otimes r_X) \circ l_X$$

$$r_{1 \otimes X} \circ l_X = (l_X \otimes \text{id}_1) \otimes r_X$$

Since l is a natural transformation one has for all morphisms $f : X \rightarrow Y$ the following commutative diagram:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ l_X \downarrow & & \downarrow l_Y \\ 1 \otimes X & \xrightarrow{\text{id}_1 \otimes f} & 1 \otimes Y \end{array}$$

Writing $Y = 1 \otimes X$ and $f = l_X$ we get

$$\begin{array}{ccc} X & \xrightarrow{l_X} & 1 \otimes X \\ l_X \downarrow & & \downarrow l_{1 \otimes X} \\ 1 \otimes X & \xrightarrow{\text{id}_1 \otimes l_X} & 1 \otimes (1 \otimes X) \end{array}$$

i.e.

$$l_{1 \otimes X} \circ l_X = (\text{id}_1 \otimes l_X) \circ l_X$$

since l_X is an isomorphism, this yields:

$$l_{1 \otimes X} = \text{id}_1 \otimes l_X$$

writing $f = r_X$ gives:

$$\begin{array}{ccc} X & \xrightarrow{r_X} & X \otimes 1 \\ l_X \downarrow & & \downarrow l_{X \otimes 1} \\ 1 \otimes X & \xrightarrow{\text{id}_1 \otimes r_X} & 1 \otimes (X \otimes 1) \end{array}$$

i.e.

$$l_{X \otimes 1} \circ r_X = (\text{id}_1 \otimes r_X) \circ l_X$$

Similarly one obtains that

$$r_{X \otimes 1} = r_X \otimes \text{id}_1$$

and

$$r_{1 \otimes X} \circ l_X = (l_X \otimes \text{id}_1) \circ r_X$$

from the commutativity of the diagram:

$$\begin{array}{ccc} X & \xrightarrow{l_X} & 1 \otimes X \\ r_X \downarrow & & \downarrow r_{1 \otimes X} \\ X \otimes 1 & \xrightarrow{l_X \otimes \text{id}_1} & (1 \otimes X) \otimes 1 \end{array}$$

Remark This is in contradiction with Saavedra. on page 19:

$$l_{X \otimes 1} = l_X \otimes \text{id}_1$$

and

$$r_{1 \otimes X} = \text{id}_1 \otimes r_X$$

But it seems that these are wrong.

Lemma 43 *If Z is isomorphic to 1 by a morphism $z : Z \rightarrow 1$, then one has the following*

commutative diagram:

$$\begin{array}{ccc}
 & Z \otimes Z & \\
 \text{id}_Z \otimes z \swarrow & & \searrow z \otimes \text{id}_Z \\
 Z \otimes 1 & & 1 \otimes Z \\
 r_Z \swarrow & & \searrow l_Z \\
 & Z &
 \end{array}$$

Naturality of l gives

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y \\
 l_X \downarrow & & \downarrow l_Y \\
 1 \otimes X & \xrightarrow{\text{id}_1 \otimes f} & 1 \otimes Y
 \end{array}$$

Writing $X = Z$, $Y = 1$, and $f = z$ gives:

$$\begin{array}{ccc}
 Z & \xrightarrow{z} & 1 \\
 l_Z \downarrow & & \downarrow l_1 \\
 1 \otimes Z & \xrightarrow{\text{id}_1 \otimes z} & 1 \otimes 1
 \end{array}$$

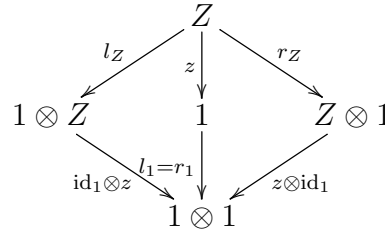
Naturality of r gives

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y \\
 r_X \downarrow & & \downarrow r_Y \\
 X \otimes 1 & \xrightarrow{\text{id}_1 \otimes f} & Y \otimes 1
 \end{array}$$

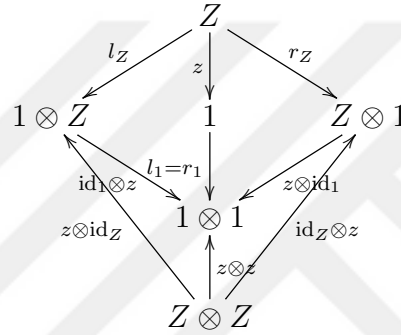
Writing $X = Z$, $Y = 1$ and $f = z$ gives:

$$\begin{array}{ccc}
 Z & \xrightarrow{z} & 1 \\
 r_Z \downarrow & & \downarrow r_1 \\
 Z \otimes 1 & \xrightarrow{\text{id}_1 \otimes z} & 1 \otimes 1
 \end{array}$$

Since $r_1 = l_1$ this gives



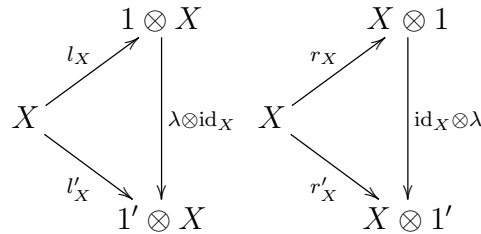
One may complete this diagram by



Remark

One may define left and right units only by couples $(1, l)$ or $(1, r)$ instead of the bilateral unit defined here by the triple $(1, l, r)$.

Definition 131 A morphism of units $(1, l, r)$ and $(1', l', r')$ is a morphism $\lambda : 1 \rightarrow 1'$ making the following diagrams commute:



Lemma 44 A morphism of units λ is an isomorphism. λ is uniquely determined and

$$\lambda = r_{1'}^{-1} \circ l'_1 = l_1^{-1} \circ r'_1$$

By taking $X = 1$ one gets:

$$\begin{array}{ccccc}
 & & 1 \otimes 1 & & \\
 & \swarrow \text{id}_1 \otimes \lambda & \uparrow l_1 = r_1 & \searrow \lambda \otimes \text{id}_1 & \\
 1 \otimes 1' & \xleftarrow{r'_1} & 1 & \xrightarrow{l'_1} & 1' \otimes 1
 \end{array}$$

Since $(\lambda \otimes \text{id}_1) \circ r = l'_1$ and $r = l_1 = r_1$ and l'_1 are isomorphisms, $\lambda \otimes \text{id}_1$ is an isomorphism.

Since

$$\begin{array}{ccc}
 1 & \xrightarrow{\lambda} & 1' \\
 r_1 \downarrow & & \downarrow r_{1'} \\
 1 \otimes 1 & \xrightarrow{\lambda \otimes \text{id}_1} & 1' \otimes 1
 \end{array}$$

and $r_1 = l_1 = r$ and $r_{1'}$ are isomorphisms, so is λ .

Considering the diagram:

$$\begin{array}{ccc}
 1 & \xrightarrow{\lambda} & 1' \\
 r_1 \downarrow & & \downarrow r_{1'} \\
 1 \otimes 1 & \xrightarrow{\lambda \otimes \text{id}_1} & 1' \otimes 1 \\
 & \nwarrow l_1 = r_1 & \nearrow l'_1 \\
 & 1 &
 \end{array}$$

Note that λ is uniquely determined:

$$\lambda = r_{1'}^{-1} \circ l'_1 \circ l_1^{-1} \circ r_1 = r_{1'}^{-1} \circ l'_1$$

One can also form the diagram

$$\begin{array}{ccc}
 1 & \xrightarrow{\lambda} & 1' \\
 l_1 \downarrow & & \downarrow l_{1'} \\
 1 \otimes 1 & \xrightarrow{\text{id}_1 \otimes \lambda} & 1 \otimes 1' \\
 & \nwarrow l_1 = r_1 & \nearrow r'_1 \\
 & 1 &
 \end{array}$$

yielding that

$$\lambda = l_{1'}^{-1} \circ r'_1$$

Hence one has the commutative diagram

$$\begin{array}{ccc}
 & 1' & \\
 r_{1'} \swarrow & & \searrow l_{1'} \\
 1' \otimes 1 & & 1 \otimes 1' \\
 l'_1 \swarrow & & \searrow r_1 \\
 & 1 &
 \end{array}$$

Definition 132 Let $\mathbf{C}$ be a tensor category.

- An object 1 of $\mathbf{C}$ is said to be a unit object if it is 2-regular, and there exists an isomorphism $1 \cong 1 \otimes 1$
- A couple $(1, r)$ where $r : 1 \xrightarrow{\sim} 1 \otimes 1$ is such an isomorphism is called a reduced unit for $\mathbf{C}$
- A tensor category $\mathbf{C}$ is said to be unital if it has a unit object.

Remark Note that if $(1, l, r)$ is a unit constraint for a tensor category $\mathbf{C}$ then $(1, r_1)$ is a reduced unit.

Lemma 45 If a tensor category $\mathbf{C}$ has an associativity constraint, then $\mathbf{C}$ is unital if and only if there exists a unit object and any two unit objects are isomorphic.

Clearly if there exists a unit object, then $\mathbf{C}$ is unital by definition. On the other hand suppose $\mathbf{C}$ is unital and 1 and $1'$ are both unit objects. Then $1 \cong 1 \otimes 1$ and $1' \cong 1' \otimes 1'$, via isomorphisms called r and r' respectively.

Then one has the isomorphisms:

$$1 \otimes (1 \otimes 1') \xrightarrow{\phi} (1 \otimes 1) \otimes 1' \xrightarrow{r^{-1} \otimes \text{id}_{1'}} 1 \otimes 1' \xrightarrow{\text{id}_1 \otimes r'} 1 \otimes (1' \otimes 1')$$

where ϕ is the constraint of associativity.

Now because tensoring with 1 on the left is an equivalence of categories, $1 \otimes 1'$ ends up being isomorphic to $1' \otimes 1'$, and since tensoring with $1'$ on the right is an equivalence of categories, $1 \cong 1'$.

Definition 133 A morphism of reduced units $(1, r)$ and $(1', r')$ is an isomorphism $\lambda : 1 \rightarrow 1'$

that makes the following diagram commute:

$$\begin{array}{ccc} 1 & \xrightarrow{r} & 1 \otimes 1 \\ \lambda \downarrow & & \downarrow \lambda \otimes \lambda \\ 1' & \xrightarrow{r'} & 1' \otimes 1' \end{array}$$

Lemma 46 *The functor from unit constraints on a tensor category to reduced units on the same category, which maps a unit constraint $(1, l, r)$ to the reduced unit $(1, r_1)$ defines a fully faithful functor. This is not in general an equivalence of categories.*

Lemma 47 *For a unit object of a tensor category $\mathbf{C}$, the monoid of endomorphisms of the unit object, denoted by $\text{End}(1)$ is commutative.*

Remark

It suffices to prove that $\text{End}(1 \otimes 1)$ is commutative, and two-regularity of 1 implies that all such endomorphisms can be expressed as $u \otimes \text{id}_1 = \text{id}_1 \otimes v$ for $u, v \in \text{End}(1)$. The commutativity then follows by direct computation.

Lemma 48 *Isomorphisms of unit objects define an isomorphism of their endomorphism monoids. This is independent of the chosen isomorphism among the unit objects.*

In particular, if a tensor category is unital where all unit objects are isomorphic (for example in the case that there is an associativity constraint), one may define without ambiguity, the endomorphism monoid of unit object, denoted by $\text{End}(1_{\mathbf{C}})$.

Lemma 49 *Let $\mathbf{C}$ be a tensor category with a unit constraint $(1, l, r)$. There are two maps*

$$\rho^l, \rho^r : \text{End}(1) \rightarrow \text{End}(\text{id}_{\mathbf{C}})$$

such that for each $u \in \text{End}(1)$ and $X \in \text{Ob}(\mathbf{C})$, there are morphisms

$$\rho_X^l(u), \rho_X^r(u) : X \rightarrow X$$

defined by the following commutative diagrams:

$$\begin{array}{ccc} X & \xrightarrow{\rho_X^l(u)} & X \\ l_X \downarrow & & \downarrow l_X \\ 1 \otimes X & \xrightarrow{u \otimes \text{id}_X} & 1 \otimes X \end{array} \quad \begin{array}{ccc} X & \xrightarrow{\rho_X^r(u)} & X \\ r_X \downarrow & & \downarrow r_X \\ 1 \otimes X & \xrightarrow{u \otimes \text{id}_X} & 1 \otimes X \end{array}$$

These preserve the operation of the monoids. In other words for $u, v \in \text{End}(1)$ one has

$$\rho_X^l(uv) = \rho_X^l(u)\rho_X^l(v) \rho_X^l(\text{id}_1) = \text{id}_X$$

and

$$\rho_X^r(uv) = \rho_X^r(u)\rho_X^r(v) \rho_X^r(\text{id}_1) = \text{id}_X$$

$\rho_X^l(u)$ and $\rho_X^r(u)$ are natural in X and by naturality of r ,

$$\rho_1^l(u) = \rho_1^r(u) = u$$

Consequently, the monoid $\text{End}(\text{id}_C)$ is commutative, ρ_X^l and ρ_X^r commute for all objects X .

4.5. COMPATIBILITY AMONG CONSTRAINTS

Compatibility conditions arise, when one can go from an object to another object via a sequence of morphisms pieced together by the constraint morphisms and identity morphisms and the tensor functor, in different ways, and the resulting morphisms should be equalities.

4.5.1. Associativity and Commutativity

$(X \otimes Y) \otimes Z \cong X \otimes (Y \otimes Z)$ under associativity constraint.

And $(X \otimes Y) \otimes Z \cong Z \otimes (X \otimes Y)$ under commutativity constraint, and

$(X \otimes Y) \otimes Z \cong (Y \otimes X) \otimes Z$ under tensor of commutativity constraint with identity on Z .

Repeating this in all other rearrangements of X, Y, Z and piecing together ones that fit into a commutative diagram, in one commutative diagram, yields a commutative hexagon, formed from two sequences of three morphisms:

$$X \otimes (Y \otimes Z) \xrightarrow{\text{assoc}} (X \otimes Y) \otimes Z \xrightarrow{\text{comm}} Z \otimes (X \otimes Y) \xrightarrow{\text{assoc}} (Z \otimes X) \otimes Y$$

and

$$X \otimes (Y \otimes Z) \xrightarrow{\text{id} \otimes \text{comm}} X \otimes (Z \otimes Y) \xrightarrow{\text{assoc}} (X \otimes Z) \otimes Y \xrightarrow{\text{comm} \otimes \text{id}} (Z \otimes X) \otimes Y$$

Since these start and end at the same object, the compatibility constraint is that these two sequences combine to fit into a commutative hexagon.

Definition 134 Let $\mathbf{C}$ be a tensor category. An associativity constraint φ and a commutativity constraint Ψ are said to be compatible if the following diagram commutes:

$$\begin{array}{ccccc}
 & & (X \otimes Y) \otimes Z & \xrightarrow{\Psi_{X \otimes Y, Z}} & Z \otimes (X \otimes Y) \\
 & \nearrow \varphi_{X, Y, Z} & & & \searrow \varphi_{Z, X, Y} \\
 X \otimes (Y \otimes Z) & & & & (Z \otimes X) \otimes Y \\
 & \searrow \text{id}_X \otimes \Psi_{Y, Z} & & & \nearrow \Psi_{X, Z} \otimes \text{id}_Y \\
 & & X \otimes (Z \otimes Y) & \xrightarrow{\varphi_{X, Z, Y}} & (X \otimes Z) \otimes Y
 \end{array}$$

In such a case $(\mathbf{C}, \otimes, \varphi, \Psi)$ is said to be an AC-tensor category. It is strict if Ψ is.

4.5.1.1. Remark on Associativity and Commutativity Constraint

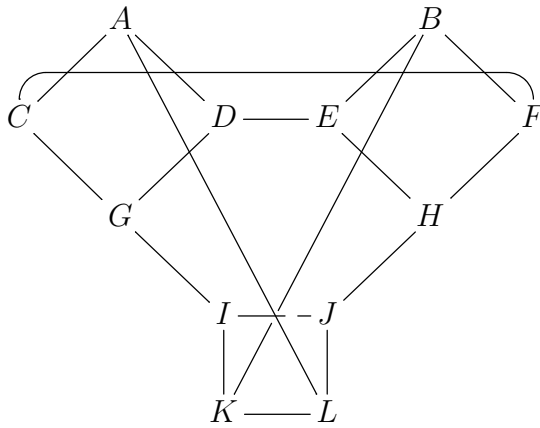
This piece concerns the compatibility constraints between associativity and commutativity constraints on tensor categories. In particular it concerns associativity and commutativity constraint.

In this commutative diagram a is an associativity constraint(isomorphism), and c is a commutativity constraint(isomorphism).

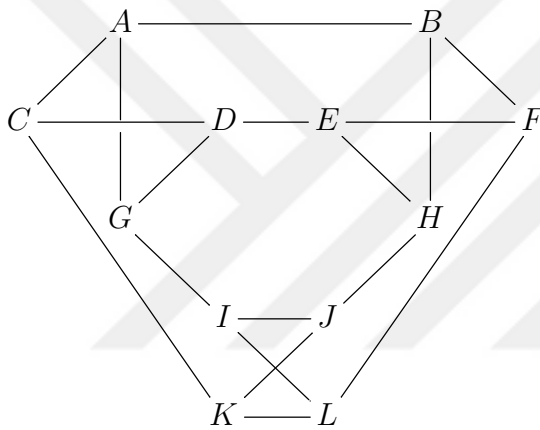
Concerning the first diagram:

Note that because the morphisms in the diagram are all isomorphisms, hence arrows can be chosen in either direction in forming a commutative subdiagram. The choice of direction for associativity constraints, though can be chosen in two distinct ways. The directions for commutativity constraints were chosen so that the main inner and outside hexagon enforce commutativity of three arrows chosen in sequence. (Other choices would lead to unbalanced constraints, meaning not composition of three arrows equaling composition of three other arrows, but possibly composition of five arrows to one arrow or four arrows to two arrows. They would not indicate a different condition than the one currently imposed as the associativity-commutativity constraint. Also it is possible to form other hexagons by traversing the graph above through different routes. However, as it is discussed below, all hexagons in this diagram fall under the action of S_3 acting on the graph, by permuting the objects X, Y, Z . S_3 acts on these hexagons (though not transitively). However there are other hexagons that do not fall in this class of hexagons, so called non-standard hexagons. These other hexagons, are obtained by gluing two hexagons together. Their edges do not obey the rule of associativity alternating with commutativity along the edges. In conclusion, all possible hexagonal diagrams are obtained from only a single hexagon choice as a commutative diagram basis. The reason for choice of a hexagon, is that starting at one of the objects in the diagram, (apart from the three squares that are formed from solely commutativity constraints – which is assumed) one can come back to the same object by traversing a path that contains both commutativity and associativity constraints shortest in six steps.

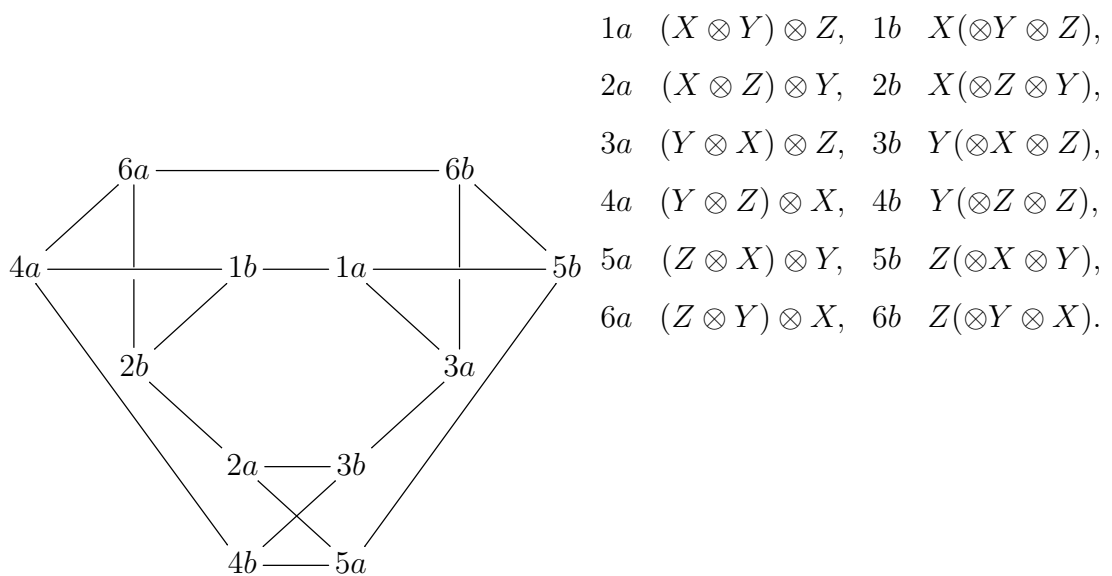
Diagrams redrawn



The full associativity commutativity diagram - First form



The full associativity commutativity diagram - Second form



Arguments

Three symbols X, Y, Z can be permuted, arranged in $3! = 6$ ways. In combining the symbols via a binary operation, a single sequence of three letters can be put in operation in 2 ways, due to choice of parantheses' placement. Associativity condition requires these two ways to be equal (in this case isomorphic) to each other. In total, from a choice of three objects in our category, we obtain via (tensor) product, twelve objects that are in the diagrams in previous section. These twelve points can be placed in three squares using commutativity constraints (isomorphisms). The diagrams were drawn keeping these points in mind. What is referred as the associativity-commutativity constraint is the innermost (alternatively outermost) hexagon in the diagram, that is formed by alternating associativity and commutativity isomorphisms. [Insert associativity-commutativity hexagon here.]

One possible question on the diagram is how many hexagons are there?

Lemma 50 *Every square edge appears in two (three) hexagons.*

Proof 4 *Because starting with a square edge (i.e. commutativity constraint), skipping to associative edges leads one to "opposite points" on a hexagons. "Opposite points" (those of distance three on the graph, when forced to traverse by alternating edge type from associativity to commutativity or from commutativity to associativity) can be joined in three distinct routes of length three. Two of those routes start with square edge (commutativity constraint). Hence there are two hexagons with alternating edges one hexagon with "mirror" edge pattern.*

- There are three squares hence there $3 \times 4 = 12$ commutativity edges.
- Each hexagon contains 3 of these edges.
- Number of hexagons obeying the alternation rule is $2 \times 12/3 = 8$.

Fixing a type of hexagon not obeying the path alternation rule. Here we specifically define the path alternation rule.

Definition 135 *A path in the diagram is said to obey the alternation rule, if each associativity edge is (if preceded by some edge) is preceded by a commutativity edge and (if superceded/followed by some edge) is superceded by a commutativity edge, and vice versa.*

The hexagons that do not obey the alternation rule, can each be obtained by combining two hexagons that share an alternating path of length three, and omitting that path. For that to happen two hexagons must share two of the three numbers corresponding to edges/vertices they contain. Each hexagon shares two numbers with $C(3, 2) = 3$ other ones. Each gluing gives a new hexagon of other type. This gives $8 \times 3/2 = 12$ hexagons of other type. (Dividing by two since new hexagons are formed from pairs of old hexagons, so each new hexagon is counted twice.)

Listing of hexagons: We follow the convention listed in the diagram of specifying vertices with a number one through six followed by a letter a or b.

Eight hexagons that obey the path alternation rule are listed below.

- IA : vertex order $\{4a, 1b, 1a, 3a, 3b, 4b\}$ numbers listed $\{1, 3, 4\}$

- IB : vertex order $\{4a, 6a, 6b, 3a, 3b, 4b\}$ numbers listed $\{3, 4, 6\}$
- IIA : vertex order $\{4a, 1b, 1a, 5b, 5a, 4b\}$ numbers listed $\{1, 4, 5\}$
- IIIA: vertex order $\{2b, 2a, 5a, 5b, 1a, 1b\}$ numbers listed $\{1, 2, 5\}$
- IIIB: vertex order $\{2b, 2a, 5a, 5b, 6b, 6a\}$ numbers listed $\{2, 5, 6\}$
- IVA: vertex order $\{2b, 2a, 3b, 3a, 1a, 1b\}$ numbers listed $\{1, 2, 3\}$
- IVB: vertex order $\{2b, 2a, 3b, 3a, 6b, 6a\}$ numbers listed $\{2, 3, 6\}$

Four of the twelve hexagons that do not obey the path alternation rule (omitting because of length, maybe fill them in later) path alternating is violated at the first and fourth vertex.

- IC: vertex order $\{4a, 6a, 6b, 3a, 1a, 1b\}$ numbers listed $\{1, 6\}$ those numbers for which only a single letter is present : $\{4a, 3a\}$
- IIC: vertex order $\{4a, 6a, 6b, 5b, 1a, 1b\}$ numbers listed $\{1, 6\}$ those numbers for which only a single letter is present : $\{4a, 5b\}$
- IIIC: vertex order $\{2b, 6a, 6b, 5b, 1a, 1b\}$ numbers listed $\{1, 6\}$ those numbers for which only a single letter is present: $\{2b, 5b\}$
- IVC: vertex order $\{2b, 6a, 6b, 3a, 1a, 1b\}$ numbers listed $\{1, 6\}$ those numbers for which only a single letter is present: $\{2b, 3a\}$

Action of S_3 on letter sequences, hence hexagons, and vertices.

Let V_i denote $\{ia, ib\}$ for $i = 1, \dots, 6$.

Let $(12)(X, Y, Z) = (Y, X, Z)$ and $(123)(X, Y, Z) = (Y, Z, X)$ be the action of S_3 on ordered symbols.

Then Under action of (12) $\{V_1, V_3\}$ and $\{V_2, V_4\}$ and $\{V_5, V_6\}$ are switched. Under action of (123) $V_1 \mapsto V_4 \mapsto V_5 \mapsto V_1$ and $V_2 \mapsto V_3 \mapsto V_6 \mapsto V_2$ For completeness Under action of (23) $\{V_1, V_2\}$ $\{V_3, V_5\}$ and $\{V_4, V_6\}$ are interchanged. Under action of (13) $\{V_1, V_6\}$ $\{V_2, V_5\}$ and $\{V_3, V_4\}$ are interchanged.

Action on hexagons:

Action of (12)

$$IA \leftrightarrow IVA, IB \leftrightarrow IIIA, IIA \leftrightarrow IVB, IIB \leftrightarrow IIIB$$

Action of (23)

$$IA \leftrightarrow IIIB, IB \leftrightarrow IIB, IIA \leftrightarrow IVB, IIIA \leftrightarrow IVA$$

Transitivity of action fails. There are two orbits for hexagons, one of size six, and another of size two. Orbit 1

$$IA \xrightarrow{(12)} IVA \xrightarrow{(23)} IIIA \xrightarrow{(12)} IB \xrightarrow{(23)} IIB \xrightarrow{(12)} IIIB \xrightarrow{(23)} IA$$

Orbit 2

$$IIA \xrightarrow{(12) \text{ or } (23)} IVB$$

4.5.2. Associativity and Unit

$(X \otimes Y) \cong (X \otimes Y) \otimes 1 \cong X \otimes (Y \otimes 1) \cong X \otimes Y$ which gives a commutative triangle.

And three other sequences formed from rearrangement of the objects $X, Y, 1$

Definition 136 For a tensor category $\mathbf{C}$ an associativity constraint φ and a unit constraint $(1, l, r)$ are said to be compatible if the following three triangles commute:

$$\begin{array}{ccc} X \otimes (Y \otimes 1) & \xrightarrow{\varphi_{X,Y,1}} & (X \otimes Y) \otimes 1 \\ & \swarrow \text{id}_X \otimes r_Y & \searrow r_{X \otimes Y} \\ & X \otimes Y & \end{array}$$

$$\begin{array}{ccc} 1 \otimes (X \otimes Y) & \xrightarrow{\varphi_{1,X,Y}} & (1 \otimes X) \otimes Y \\ & \swarrow l_{X \otimes Y} & \searrow l_X \otimes \text{id}_Y \\ & X \otimes Y & \end{array}$$

$$\begin{array}{ccc} X \otimes (1 \otimes Y) & \xrightarrow{\varphi_{X,1,Y}} & (X \otimes 1) \otimes Y \\ & \swarrow \text{id}_X \otimes l_Y & \searrow r_X \otimes \text{id}_Y \\ & X \otimes Y & \end{array}$$

The pair $(\varphi, (1, l, r))$ is called an AU constraint for the tensor category $\mathbf{C}$ and the category is called an AU-tensor-category.

Lemma 51 *The third diagram follows from the first two in compatibility among associativity and unit.*

Remark

The following two diagrams give the minimal condition for establishing that associativity and unit constraints are compatible. (Reference given to [50].) For related other questions: [64], [52].

$$\begin{array}{ccc}
 X \otimes (1 \otimes 1) & \xrightarrow{\varphi_{X,1,1}} & (X \otimes 1) \otimes 1 \\
 \swarrow \text{id}_X \otimes r_1 & & \nearrow r_{X \otimes 1} \\
 & X \otimes 1 & \\
 \\
 1 \otimes (1 \otimes Y) & \xrightarrow{\varphi_{1,1,Y}} & (1 \otimes 1) \otimes Y \\
 \swarrow l_{1 \otimes Y} & & \nearrow l_1 \otimes \text{id}_Y \\
 & 1 \otimes Y &
 \end{array}$$

Definition 137 *For a tensor category $\mathbf{C}$, $\text{Unit}(\mathbf{C})$ is the category whose objects are units (unit constraints) $(1, l, r)$, whose morphisms are unit-morphisms. Given an associativity constraint φ , the category $\text{UA}_\varphi(\mathbf{C})$ is the plain subcategory of $\text{Unit}(\mathbf{C})$ whose objects are unit constraints that are compatible with φ .*

Proposition 5 *The rigid groupoid $\text{UA}_\varphi(\mathbf{C})$ is trivial. Any two of its objects are isomorphic, and the morphisms from a unit constraint to another is a single element set.*

(A groupoid is a category in which all morphisms are isomorphisms. It is rigid, if each hom set has a single element.)

Definition 138 *Let $\text{RU}(\mathbf{C})$ denote the category of reduced units, i.e. the category whose objects are pairs $(1, r)$ of a unit object 1 and an isomorphism $r : 1 \xrightarrow{\sim} 1 \otimes 1$, and morphisms*

are morphisms $\lambda : 1 \rightarrow 1'$ such that

$$\begin{array}{ccc} 1 & \xrightarrow{r} & 1 \otimes 1 \\ \lambda \downarrow & & \downarrow \lambda \otimes \lambda \\ 1' & \xrightarrow{r'} & 1' \otimes 1' \end{array}$$

satisfying this commutative diagram.

Proposition 6 *There is a functor*

$$\mathrm{UA}_\varphi(\mathbf{C}) \rightarrow \mathrm{RU}(\mathbf{C})$$

This functor is an isomorphism of categories. In particular, for all objects 1 of $\mathbf{C}$, the set of unit structures of $\mathbf{C}$ over 1 is in one-to-one correspondence with the set of isomorphisms $1 \xrightarrow{\sim} 1 \otimes 1$.

Remark

Note that given a reduced unit $(1, r_0)$ one constructs unit constraint using φ by

$$X \otimes 1 \xrightarrow{\mathrm{id}_X \otimes r_0} X \otimes (1 \otimes 1) \xrightarrow{\varphi_{X,1,1}} (X \otimes 1) \otimes 1$$

Then one may use that tensoring with 1 is an equivalence of categories to construct $r_X : X \rightarrow X \otimes 1$ from this composition.

Remark - Significance of proven result

If a tensor category is associative, then the category has a unit (constraint) compatible with associativity constraint if and only if it possesses a unit object.

A choice $(1, l, r)$ is such a unit, depends on the choice of unit object 1 and the isomorphism $l_1 = r_1 : 1 \xrightarrow{\sim} 1 \otimes 1$, and these units are canonically isomorphic among each other.

4.5.3. Commutativity and Unit

Unit constraint $(1, l, r)$ consists of morphisms $r : X \rightarrow X \times 1$ and $l : X \rightarrow 1 \times X$. Commutativity constraint gives a morphism $\Psi_{X,1} : X \times 1 \rightarrow 1 \times X$. The compatibility among them is given by a commuting triangle: $X \cong X \otimes 1 \cong 1 \otimes X \cong X$

Definition 139 *For a tensor category $\mathbf{C}$, a commutativity constraint Ψ and a unit constraint*

$(1, l, r)$ are said to be compatible if the following triangle:

$$\begin{array}{ccc}
 & X \otimes 1 & \\
 l_X \nearrow & & \downarrow \Psi_{X,1} \\
 X & & \\
 r_X \searrow & & \\
 & 1 \otimes X &
 \end{array}$$

is commutative, i.e.

$$r_X = \Psi_{X,1} \circ l_X$$

In particular $\Psi_{1,1} = \text{id}_{1 \otimes 1}$. The pair $(\Psi, (1, l, r))$ is called a CU constraint, and $\mathbf{C}$ is called a CU tensor category.

4.5.4. Associativity, Commutativity and Unit

Definition 140 A triplet $(\varphi, \Psi, (1, l, r))$ consisting of an associativity constraint φ , a commutativity constraint Ψ and a unit constraint $(1, l, r)$ on a tensor category $\mathbf{C}$ are said to be compatible if they are pairwise compatible. Such a triplet is called an ACU constraint, and such a category is called an ACU tensor category. It is strict if Ψ is.

Proposition 7 AC and AU implies CU.

4.6. INVERTIBLE OBJECTS

Definition 141 If $\mathbf{C}$ is an associative $\otimes$ -category, one says that an object X of $\mathbf{C}$ is invertible if it is 2-regular.

Lemma 52 An object is invertible if and only if there exists an object X' such that $X \otimes X'$ and $X' \otimes X$ are unit objects.

Definition 142 An inverse of X is a pair (X^{-1}, δ) where $\delta : X \otimes X^{-1} \xrightarrow{\sim} 1$ where 1 is the identity object.

4.7. TANNAKIAN CATEGORIES

4.7.1. Internal Hom

Definition 143 *If the contravariant functor $T \mapsto \text{Hom}(T \otimes X, Y)$ is representable, $\underline{\text{Hom}}(X, Y)$ denotes the representing object. It is called the internal hom functor.*

$\text{ev}_{X,Y} : \underline{\text{Hom}}(X, Y) \otimes X \rightarrow Y$ is the morphism corresponding to $\text{id}_{\underline{\text{Hom}}(X,Y)}$ in the following sense:

Let $F_{X,Y} : \mathbf{C} \rightarrow \text{Set}$ be the functor defined by

$$F_{X,Y}(T) = \text{Hom}_{\mathbf{C}}(T \otimes X, Y)$$

and if $f : S \rightarrow T$ is a morphism, then

$$F_{X,Y}(f) : \text{Hom}_{\mathbf{C}}(T \otimes X, Y) \rightarrow \text{Hom}_{\mathbf{C}}(S \otimes X, Y)$$

defined by

$$F_{X,Y}(f)(\phi) = \phi \circ (f \otimes \text{id}_X)$$

If

$$F_{X,Y}(T) \cong \text{Hom}_{\mathbf{C}}(T, \underline{\text{Hom}}(X, Y))$$

($F_{X,Y}$ is representable with $\underline{\text{Hom}}(X, Y)$ being the representing object), and say $G_{X,Y}(T)$ is the right hand side, then

$$G_{X,Y}(f) : G_{X,Y}(T) \rightarrow G_{X,Y}(S)$$

is defined by

$$G_{X,Y}(f)(\phi) = \phi \circ f$$

for $\phi \in \text{Hom}_{\mathbf{C}}(T, \underline{\text{Hom}}(X, Y))$.

Now if we denote by $\eta_{X,Y}(T) : F_{X,Y}(T) \rightarrow G_{X,Y}(T)$ the natural transformation from F to

G (or natural equivalence), then

$$\text{ev}_{X,Y} = \eta_{X,Y}(\underline{\text{Hom}}(X, Y))^{-1}(\text{id}_{\underline{\text{Hom}}(X, Y)})$$

Lemma 53 *To $g \in \text{Hom}(T \otimes X, Y)$ there corresponds a unique $f \in \text{Hom}(T, \underline{\text{Hom}}(X, Y))$ such that*

$$\text{ev}_{X,Y} \circ (f \otimes \text{id}_X) = g$$

. i.e.

$$\begin{array}{ccc} T & \xrightarrow{\quad f \quad} & \underline{\text{Hom}}(X, Y) \\ \downarrow f & & \downarrow \text{pre}_f \\ \underline{\text{Hom}}(X, Y) & & \underline{\text{Hom}}(X, Y) \end{array} \quad \text{corresponds to} \quad \begin{array}{ccc} T \otimes X & \xrightarrow{\quad f \otimes \text{id}_X \quad} & \underline{\text{Hom}}(X, Y) \otimes X \\ \downarrow f \otimes \text{id}_X & \searrow g & \downarrow \text{ev}_{X,Y} \\ \underline{\text{Hom}}(X, Y) \otimes X & \xrightarrow{\quad \text{ev}_{X,Y} \quad} & Y \end{array}$$

Continuing the notation above, $\eta_{X,Y}(T) : \text{Hom}_{\mathbf{C}}(T \otimes X, Y) \rightarrow \text{Hom}_{\mathbf{C}}(T, \underline{\text{Hom}}(X, Y))$

Hence $f = \eta_{X,Y}(T)(g)$. Now use naturality of $\eta_{X,Y}$ for the morphism $f : T \rightarrow \underline{\text{Hom}}(X, Y)$

$$\begin{array}{ccc} \text{Hom}(\underline{\text{Hom}}(X, Y) \otimes X, Y) & \xrightarrow{\eta_{X,Y}(\underline{\text{Hom}}(X, Y))} & \text{Hom}(\underline{\text{Hom}}(X, Y), \underline{\text{Hom}}(X, Y)) \\ \downarrow \text{pre}_{f \otimes \text{id}_X} & & \downarrow \text{pre}_f \\ \text{Hom}(T \otimes X, Y) & \xrightarrow{\eta_{X,Y}(T)} & \text{Hom}(T, \underline{\text{Hom}}(X, Y)) \end{array}$$

To recognize that this is nothing but naturality of η let's rewrite above as:

$$\begin{array}{ccc} F_{X,Y}(\underline{\text{Hom}}(X, Y)) & \xrightarrow{\eta_{X,Y}(\underline{\text{Hom}}(X, Y))} & G_{X,Y}(\underline{\text{Hom}}(X, Y)) \\ \downarrow F_{X,Y}(f) & & \downarrow G_{X,Y}(f) \\ F_{X,Y}(T) & \xrightarrow{\eta_{X,Y}(T)} & G_{X,Y}(T) \end{array}$$

with F and G having the meanings defined before.

Note $G_{X,Y}(f) = \text{pre}_f$ meaning precomposing with f , and $F_{X,Y}(f) = \text{pre}_{f \otimes \text{id}_X}$ meaning precomposing with $f \otimes \text{id}_X$.

Now use the commutativity of this diagram, evaluated at $\text{ev}_{X,Y}$ to get

$$\text{pre}_f \circ \eta_{X,Y}(\underline{\text{Hom}}(X, Y)) = \eta_{X,Y}(T) \circ \text{pre}_{f \otimes \text{id}_X}$$

$$\text{pre}_f \circ \eta_{X,Y}(\underline{\text{Hom}}(X, Y))(\text{ev}_{X,Y}) = \eta_{X,Y}(T) \circ \text{pre}_{f \otimes \text{id}_X}(\text{ev}_{X,Y})$$

But by definition of $\text{ev}_{X,Y}$ we have

$$\eta_{X,Y}(\underline{\text{Hom}}(X, Y))(\text{ev}_{X,Y}) = \text{id}_{\underline{\text{Hom}}(X,Y)}$$

so

$$\text{pre}_f(\text{id}_{\underline{\text{Hom}}(X,Y)}) = \eta_{X,Y}(T)(\text{ev}_{X,Y} \circ (f \otimes \text{id}_X))$$

i.e.

$$f = \eta_{X,Y}(T)(\text{ev}_{X,Y} \circ (f \otimes \text{id}_X))$$

Since $f = \eta_{X,Y}(T)(g)$

$$\eta_{X,Y}(T)(g) = \eta_{X,Y}(T)(\text{ev}_{X,Y} \circ (f \otimes \text{id}_X))$$

Since $\eta_{X,Y}(T)$ is an isomorphism ($\eta_{X,Y}$ is a natural equivalence)

$$g = \text{ev}_{X,Y} \circ (f \otimes \text{id}_X)$$

Lemma 54 $\text{Hom}(Z, \underline{\text{Hom}}(X, Y)) \rightarrow \text{Hom}(Z \otimes X, Y)$ defined by $f \mapsto \text{ev}_{X,Y} \circ (f \otimes \text{id}_X)$ is a bijection.

This is more or less a restatement of previous lemma, with the observation that $\eta_{X,Y}(T)$ is a natural equivalence. In fact $\eta_{X,Y}(T)^{-1}(f) = \text{ev}_{X,Y} \circ (f \otimes \text{id}_X)$ by above.

Lemma 55 Internal hom defines a functor, if it is defined for all pairs of objects.

Using the first lemma of this section, corresponding to each morphism $f : X' \rightarrow X$ one can find a morphism (via the natural equivalence between $\text{Hom}(T \otimes X, Y)$ and $\text{Hom}(T, \underline{\text{Hom}}(X, Y))$) $f_* : \underline{\text{Hom}}(X, Y) \rightarrow \underline{\text{Hom}}(X', Y)$ such that

$$\text{ev}_{X',Y} \circ (f_* \otimes \text{id}_X) = \text{ev}_{X,Y} \circ (\text{id} \otimes f)$$

Similarly corresponding to each morphism $g : Y \rightarrow Y'$ one can find a morphism $g_* :$

$\underline{\text{Hom}}(X, Y) \rightarrow \underline{\text{Hom}}(X, Y')$ such that

$$\text{ev}_{X, Y'} \circ (g_*^X \otimes \text{id}_X) = h = g \circ \text{ev}_{X, Y}$$

In order to see that the functor preserves compositions, one uses the commutative diagrams formed from the definitions, and the fact that $\text{ev}_{X, Y}$ defines a bijection, stated in the previous lemma.

Definition 144

$$X^\vee = \underline{\text{Hom}}(X, 1)$$

$$\text{ev}_X = \text{ev}_{X, 1}$$

Definition 145 *Canonical morphism $i : X \rightarrow X^{\vee\vee}$ is defined by the commutative diagram:*

$$\begin{array}{ccc} X \otimes X^\vee & \xrightarrow{i_X \otimes 1} & X^{\vee\vee} \otimes X^\vee \\ \Psi_{X, X^\vee} \downarrow & & \downarrow \text{ev}_{X^\vee} \\ X^\vee \otimes X & \xrightarrow{\text{ev}_X} & 1 \end{array}$$

Note that by lemma, to $g = \text{ev}_X \circ \Psi_{X, X^\vee} \in \text{Hom}(X \otimes X^\vee, 1)$ there corresponds $i_X : X \rightarrow X^{\vee\vee}$ such that $g = \text{ev}_{X^\vee} \circ (i_X \otimes \text{id}_1)$

Definition 146 *Given a morphism $f : X \rightarrow Y$, ${}^t f : Y^\vee \rightarrow X^\vee$ is defined by the commutative diagram:*

$$\begin{array}{ccc} Y^\vee \otimes X & \xrightarrow{{}^t f \otimes 1} & X^\vee \otimes X \\ 1 \otimes f \downarrow & & \downarrow \text{ev}_X \\ Y^\vee \otimes Y & \xrightarrow{\text{ev}_Y} & 1 \end{array}$$

4.7.2. Tensor Functors

Definition 147 • A tensor functor of a tensor category $\mathbf{C}$ into a tensor category $\mathbf{C}'$ is a pair (F, c) consisting of a functor $F : \mathbf{C} \rightarrow \mathbf{C}'$ and a functorial isomorphism

$$c_{X, Y} : F(X) \otimes F(Y) \rightarrow F(X \otimes Y)$$

- (F, c) is a strict tensor functor if for all objects X, Y of $\mathbf{C}$,

$$F(X \otimes Y) = F(X) \otimes F(Y)$$

and $c_{X,Y} = \text{id}_{F(X \otimes Y)}$.

- If (F, c) and (G, d) are tensor functors a tensor morphism among the functors is a functorial morphism $\lambda : F \rightarrow G$ making the following diagram commute:

$$\begin{array}{ccc} F(X) \otimes F(Y) & \xrightarrow{c_{X,Y}} & F(X \otimes Y) \\ \lambda_X \otimes \lambda_Y \downarrow & & \downarrow \lambda_{X \otimes Y} \\ G(X) \otimes G(Y) & \xrightarrow{d_{X,Y}} & G(X \otimes Y) \end{array}$$

- Tensor morphisms, under composition, form a category called $\text{Hom}^\otimes(\mathbf{C}, \mathbf{C}')$.
- The set of tensor morphisms from F to G , $\text{Hom}((F, c), (G, d))$ is denoted by $\text{Hom}^\otimes(F, G)$.
- Composition of (F, c) and (F', c') is defined by

$$F'' = F' \circ F$$

and

$$c'' = (F' * c) \circ (c' * (F \times F))$$

where the second statement means that

$$c''_{X,Y} = F'(c_{X,Y}) \circ c'_{F(X), F(Y)}$$

- If $(G, d) : \mathbf{C} \rightarrow \mathbf{C}'$ and $(G', d') : \mathbf{C}' \rightarrow \mathbf{C}''$ are tensor functors, and $\lambda : F \rightarrow G$ and $\lambda' : F' \rightarrow G'$ are tensor morphisms, then $\lambda' * \lambda : F'F \rightarrow G'G$ is a tensor morphism.
- $\otimes - \text{Cat}$ is the 2-category whose objects are $\otimes$ -categories (tensor categories) and whose morphisms are the categories $\text{Hom}^\otimes(\mathbf{C}, \mathbf{C}')$ of tensor functors from one tensor category into another.
- A tensor functor is A -linear if the functor is.

Definition 148 • A tensor functor $(F, c) : \mathbf{C} \rightarrow \mathbf{C}'$ is compatible with associativity

constraints φ, φ' of $\mathbf{C}$ and $\mathbf{C}'$ respectively if

$$\begin{array}{ccc} FX \otimes (FY \otimes FZ) & \xrightarrow{\text{id} \otimes c_{Y,Z}} & FX \otimes F(Y \otimes Z) \xrightarrow{c_{X,Y \otimes Z}} F(X \otimes (Y \otimes Z)) \\ \downarrow \varphi'_{FX, FY, FZ} & & \downarrow F\varphi_{X,Y,Z} \\ (FX \otimes FY) \otimes FZ & \xrightarrow{c_{X,Y} \otimes \text{id}} & F(X \otimes Y) \otimes FZ \xrightarrow{c_{X \otimes Y}} F((X \otimes Y) \otimes Z) \end{array}$$

is commutative. In such a case one says that F is an associative tensor functor.

- A tensor functor is compatible with commutativity constraints Ψ, Ψ' of $\mathbf{C}$ and $\mathbf{C}'$ respectively if

$$\begin{array}{ccc} FX \otimes FY & \xrightarrow{c_{X,Y}} & F(X \otimes Y) \\ \downarrow \Psi'_{FX, FY} & & \downarrow F(\Psi_{X,Y}) \\ FX \otimes FY & \xrightarrow{c_{Y,X}} & F(Y \otimes X) \end{array}$$

is commutative.

- A functor is compatible with unit constraints $(1, l, r)$ and $(1', l', r')$ if there exists a morphism $a_F : 1' \rightarrow F(1)$ making the following diagrams commute:

$$\begin{array}{ccc} FX & \xrightarrow{F(l_X)} & F(1 \otimes X) \\ \downarrow l'_{FX} & & \downarrow c_{1,X} \\ 1' \otimes FX & \xrightarrow{a_F \otimes \text{id}_{FX}} & F(1) \otimes FX \end{array}$$

$$\begin{array}{ccc} FX & \xrightarrow{F(r_X)} & F(X \otimes 1) \\ \downarrow r'_{FX} & & \downarrow c_{X,1} \\ FX \otimes 1' & \xrightarrow{\text{id}_{FX} \otimes a_F} & FX \otimes F(1) \end{array}$$

Such a functor is called unital.

- An ACU tensor functor is a tensor functor compatible with associativity, commutativity and unit constraints.

Definition 149 Let $\mathbf{C}$ and $\mathbf{C}'$ be tensor categories. A functor $F : \mathbf{C} \rightarrow \mathbf{C}'$ is said to preserve unit objects (or be compatible with unit objects) if $(1, r)$ is a unit object of $\mathbf{C}$ then $(F(1), F(r))$ is a unit object of $\mathbf{C}'$.

Lemma 56 An ACU tensor functor $(F, c) : \mathbf{C} \rightarrow \mathbf{D}$ maps inverse objects to inverse objects.

Remark The morphism $F(\text{ev}_{X,Y}) : F(\underline{\text{Hom}}(X, Y)) \otimes F(X) \rightarrow F(Y)$ gives rise to morphisms $F_{X,Y} : F(\underline{\text{Hom}}(X, Y)) \rightarrow \underline{\text{Hom}}(FX, FY)$ and $F_X : F(X^\vee) \rightarrow F(X)^\vee$

Lemma 57 Let $\mathbf{C}$ and $\mathbf{C}'$ be tensor categories and (F, c) a tensor functor from $\mathbf{C}$ into $\mathbf{C}'$. If $\underline{\text{Hom}}$ exist for X, Y and FX, FY , there exists a unique morphism

$$F_{X,Y} : F(\underline{\text{Hom}}(X, Y)) \rightarrow \underline{\text{Hom}}(FX, FY)$$

making the following diagram commute:

$$\begin{array}{ccc} F(\underline{\text{Hom}}(X, Y)) \otimes FX & \xrightarrow{F_{X,Y} \otimes \text{id}} & \underline{\text{Hom}}(FX, FY) \otimes FX \\ \downarrow c & & \downarrow \text{ev}_{FX, FY} \\ F(\underline{\text{Hom}}(X, Y) \otimes X) & \xrightarrow{F(\text{ev}_{X,Y})} & FY \end{array}$$

If $\underline{\text{Hom}}$ exist in $\mathbf{C}$ and $\mathbf{C}'$ exist, then the morphisms $F_{X,Y}$ are natural in X and Y .

Definition 150 A functor F from $\mathbf{C}$ into $\mathbf{C}'$ (as in lemma above) is compatible with $\underline{\text{Hom}}$ if $F_{X,Y}$ is an isomorphism.

Notation $\overset{\vee}{X} = X^\vee = \underline{\text{Hom}}(X, 1)$

$$\text{ev}_X = \text{ev}_{X,1}$$

4.7.3. Tensor Equivalences

Definition 151 A quadruple of tensor equivalence of a tensor category $\mathbf{C}$ and a tensor category $\mathbf{D}$ $((F, c), (G, d), \alpha, \beta)$ consists of tensor functors $(F, c) : \mathbf{C} \rightarrow \mathbf{D}$ and $(G, d) : \mathbf{D} \rightarrow \mathbf{C}$, and tensor functor isomorphisms $\alpha : \text{id}_{\mathbf{C}} \rightarrow GF$ and $\beta : \text{id}_{\mathbf{D}} \rightarrow FG$ verifying

$$(G * \beta)(\alpha * G) = \text{id}_G$$

$$(\beta * F)(F * \alpha) = \text{id}_F$$

A tensor functor $(F, c) : \mathbf{C} \rightarrow \mathbf{D}$ is said to define a tensor equivalence if such a quadruple exists.

In other words, (F, G, α, β) is an equivalence of categories, and the tensor structure on $\mathbf{C}$ and $\mathbf{D}$ are compatible under the functors via c and d respectively.

Note:

$F * \eta$ means apply the functor to the morphism defined by the natural transformation evaluated at specific objects.

$\eta * F$ means the natural transformation is to be evaluated at the objects that the functor maps them to.

i.e. $(F * \eta)_X = F(\eta_X)$ and $(\eta * F)_X = \eta_{F(X)}$ and similarly if there are more than one object.

Proposition 8 *Let $(F, c) : \mathbf{C} \rightarrow \mathbf{D}$ be a tensor functor. This is a tensor equivalence if and only if it is an equivalence of categories.*

4.7.4. Rigid Tensor Category

Definition 152 *An ACU tensor category is rigid if*

- *It possesses internal hom objects $\underline{\text{Hom}}$*
- *The canonical morphisms*

$$\underline{\text{Hom}}(X, Y) \otimes \underline{\text{Hom}}(X', Y') \rightarrow \underline{\text{Hom}}(X \otimes X', Y \otimes Y')$$

are isomorphisms

- *All objects are reflexive, i.e. the canonical morphism $i_X : X \rightarrow X^{\vee\vee}$ is an isomorphism.*

Proposition 9 *If $(F, c) : \mathbf{C} \rightarrow \mathbf{D}$ is an ACU tensor functor, and $\mathbf{C}$ and $\mathbf{D}$ are rigid, then $F_{X,Y} : F(\underline{\text{Hom}}(X, Y)) \rightarrow \underline{\text{Hom}}(FX, FY)$ is an isomorphism for all objects X, Y of $\mathbf{C}$.*

4.7.5. Neutral Tannakian Category

Definition 153 *A neutral Tannakian category over k is a rigid abelian k -linear ACU tensor category $\mathbf{C}$ for which there exists an exact faithful k -linear ACU tensor functor $\omega : \mathbf{C} \rightarrow \text{Vec}_k$. Any such functor ω is said to be a fibre functor for $\mathbf{C}$.*

Remark Any neutral Tannakian category is equivalent (in possibly many different ways) to the category of finite-dimensional representations of an affine group scheme.

4.8. REPRESENTATIONS

Let A be a commutative ring with unit, and G an A -scheme of affine groups. One notes by $\underline{\text{Rep}}(G)$ the $\text{ACU} \otimes$ -category of linear representations of G in A -modules, and $\omega^G : \underline{\text{Rep}}(G) \rightarrow \underline{\text{Mod}}(A)$ the strict $\otimes$ -functor which consist of forgetting the actions of G . (the forgetful functor).

The group G may be reconstructed as the group of $\otimes$ -automorphisms of ω^G .



5. MOTIVES AND MOTIVIC GALOIS GROUP

5.1. INTRODUCTION

The category of motives is defined in the following sources [53, 54, 48, 85, 5, 25, 48]. One motivation for defining motives is to study solutions of algebraic equations in particular under different field extensions, and to emphasize geometric nature of solutions of equations. However there are preliminary notions that should be discussed before defining motives. These are notions of algebraic cycles, and correspondences which are generalizations of rational maps between varieties. There are equivalences among algebraic cycles which are assumed to be equal or in some relationship to each other, known as standard conjectures in literature. We are in particular interested in the case when the category of motives can be defined as a Tannakian category, which basically means that it is equipped with a product that fits in with various cohomological theories. Results in Jannsen [48] means that the category of motives is a semisimple Tannakian category when algebraic cycles are considered under numerical equivalence. This section quotes [53] for the preliminary definitions and the result by Jannsen [48].

5.2. INTERSECTION THEORY AND OTHER PRELIMINARIES

The main source for intersection theory is [29] and [53].

Definition 154 *Algebraic cycle: Let X be a smooth projective k -scheme or variety. $C(X)$ is the group of algebraic cycles of X i.e. the free abelian group generated by closed integral subschemes (subvarieties) of X . This group is graded by codimension (of subscheme or subvariety) taking values between zero and dimension of X . The free abelian group of algebraic cycles of codimension r is denoted by $C^r(X)$.*

Definition 155 *Two closed integral subschemes Z, W of X are said to intersect properly if every component Y_α of $Z \cap W$ has codimension equal to the sum of the codimensions of Z and W .*

Definition 156 *The intersection product (cycle) of two closed integral subschemes Z and W of X that intersect properly is the cycle $Z \cdot W = \sum i(Z, W, Y_\alpha, X) Y_\alpha$ where the coefficients are the intersection multiplicities (of Z and W in the component Y_α inside X .)*

Note intersection multiplicities are defined in [83]. It becomes possible to define intersection product on equivalence classes of algebraic cycles.

Definition 157 A set $\{Z_t\}$ indexed by closed points of a smooth connected quasiprojective scheme T is called an algebraic family if there exists a cycle Z on $X \times T$ such that Z_t is the (intersection-theoretic) fiber over $t \in T$. Two algebraic cycles are algebraically equivalent if there is an algebraic family containing them both. Two cycles are rationally equivalent if T is the projective line.

Lemma 58 Given two cycles Z and W on a variety X there exists a variety Y rationally equivalent to W such that Z and Y intersect properly so that the intersection cycle $Z \cdot Y$ is defined.

Lemma 59 Given three cycles Z, W, Y on a variety X such that Z intersects W and Y properly, if W is rationally (algebraically) equivalent to Y , then the intersection cycles $Z \cdot W$ and $Z \cdot Y$ are rationally equivalent.

Theorem 5 Group of cycle classes of a variety X under rational (algebraic) equivalence forms a graded ring denoted by $C_{\text{rat}}(X)$ (or $C_{\text{alg}}(X)$ under the intersection product. The grading comes from codimension of subschemes, and rational equivalence classes of algebraic cycles formed from codimension r subschemes (subvarieties) is denoted by $C_{\text{rat}}^r(X)$, so that $C_{\text{rat}}(X) = \bigoplus_{r=0}^{\dim(X)} C_{\text{rat}}^r(X)$

Definition 158 Degree of an algebraic cycle in a smooth projective variety X of codimension $\dim(X)$ is defined as the sum of the coefficients. In other words if $Y \in C_{\text{rat}}^{\dim(X)}(X)$ and $Y = \sum_{\alpha} n_{\alpha} P_{\alpha}$ where P_{α} are points of X , then degree of Y is defined as $\deg(Y) = \deg(\sum_{\alpha} n_{\alpha} P_{\alpha}) = \sum_{\alpha} n_{\alpha}$

Note, in other contexts, the definition of the degree map may require the coefficients n_{α} to be multiplied by $\deg(P_{\alpha})$. See for example Hartshorne p 146.

Definition 159 Two algebraic cycles Y and W of a smooth projective variety X of same codimension are numerically equivalent if for all algebraic cycles Z of complementary codimension (i.e. of dimension $\dim(X) - \dim(Z)$, or of codimension $\dim(Z)$) the degrees

of the intersection cycles $Z \cdot Y$ and $Z \cdot W$ are the same. Algebraic cycles of a smooth projective variety under numerical equivalence are denoted by $C_{\text{num}}(X)$.

Note in Fulton's Intersection theory [29] p 374 there is an alternative definition for numerical equivalence defined through an integral. The first definition is for cycles in a complete scheme, that a cycle is numerically equivalent to zero if its integral with cap product with polynomials of Chern classes of all vector bundles is zero. If the scheme is nonsingular this is equivalent to requiring that the integral of the intersection product with all cycles of complementary dimension is zero. The second case is what is quoted above, as the integral of a zero cycle is the degree in the sense defined above.

Lemma 60 *If two cycles are rationally equivalent then they are numerically equivalent. (Rational equivalence is finer than numerical equivalence.)*

It is also possible to consider the groups/rings of algebraic cycles under equivalences formed by taking coefficients from a field F (of characteristic zero). This group is denoted by $C(X, F) = C(X) \otimes_{\mathbb{Z}} F$.

Definition 160 *Pullback and pushforward of a morphism of varieties: For a morphism $f : X \rightarrow Y$ of varieties, f induces a ring homomorphism (pullback) $f^* : C(Y) \rightarrow C(X)$ where for a closed integral subscheme W of Y $f^*(W)$ is the intersection-theoretic inverse image $f^{-1}(W)$. f also induces a ring homomorphism (pushforward) $f_* : C^p(X) \rightarrow C^{p+\dim(Y)-\dim(X)}(Y)$ defined by $f_*(Z) = [k(Z) : k(f(Z))] \overline{f(Z)}$ if $\dim(Z) = \dim(f(Z))$ and is zero if $\dim(Z) > \dim(f(Z))$.*

Note here intersection theoretic inverse image means that one takes the intersection of graph of f and inverse image of W under the projection of $X \times Y$ onto Y and pushes the intersection cycle to the first component X . See [39] page 426.

Lemma 61 *Projection formula*

$$f_*(f^*(W) \cdot Z) = W \cdot f_*(Z)$$

for proper morphisms.

Definition 161 Correspondences: A correspondence of grading r between varieties X and Y is an algebraic cycle of codimension $\dim(X) + r$ in algebraic cycles of the product variety $X \times Y$. First it is assumed that X is connected. Then this definition is generalized to the case when X has connected components X_i . These are denoted by $\text{Corr}^r(X, Y) = C^{\dim(X)+r}(X \times Y)$

Composition of correspondences: If $f \in \text{Corr}^r(X_1, X_2)$ and $g \in \text{Corr}^s(X_2, X_3)$ then their composition $g \circ f \in \text{Corr}^{r+s}(X_1, X_3)$ is defined by

$$g \circ f = (p_{13})_*(p_{12}^*f \cdot p_{23}^*g)$$

where $p_{ij} : X_1 \times X_2 \times X_3 \rightarrow X_i \times X_j$ are the projection maps, and f_* and f^* are the pullback and pushforward of a morphism of varieties.

Lemma 62 Composition of correspondences is associative.

5.3. ADEQUATE EQUIVALENCE RELATION

For this discussion a variety is a reduced scheme not necessarily irreducible. In this section and the following, we will consider smooth projective varieties over a field k .

An algebraic cycle on a variety X is a formal finite integral linear combination $Z = \sum_{\alpha} n_{\alpha} Z_{\alpha}$ of irreducible subvarieties of X . If all the Z_{α} have the same codimension i we say that Z is a codimension i cycle, and the abelian group formed by the codimension i cycles on X is denoted by $Z^i(X)$

Note that in the other section, an the group of algebraic cycles was defined as the free abelian group generated by closed integral subschemes of a smooth projective k -scheme. Since a scheme is integral if and only if reduced and irreducible, this amounts to the same definition.

If in the grading of cycles one would like to write dimension as opposed to codimension, lower indices are going to be used, so that $Z^i(X) = Z_{\dim(X)-i}(X)$. (This is valid when X is pure dimensional.)

Cartesian product of two cycles is defined via product of subvarieties.

Push-forward of a cycle under a morphism $f : X \rightarrow Y$ of k -varieties is defined as $f_*(Z) = [k(Z) : k(f(Z))]f(Z)$, intersection of subvarieties is defined as the formal sum

along the components of the intersection with coefficients equal to intersection number. (This definition requires f to be a proper morphism, so that $f(Z)$ is a closed subscheme of Y .)

Pull-back $f^*(Z) = [\text{pr}_X]_*(\Gamma_f \cdot (X \times Z))$ (there are alternative definitions for pull-back, such as $f^{-1}(Z)$ where this may be interpreted as the fibered product scheme $X \times_Y Z$ defining a cycle in X . this is for flat morphisms of a fixed relative dimension. See Fulton intersection theory)

Correspondences are cycles of the product of two varieties. Correspondences act on the cycles of the first variety, mapping them to cycles of the second variety by

$$Z(T) = [\text{pr}_Y]_*(Z \cdot (T \times Y))$$

where X and Y are two varieties, Z is a cycle of codimension t in $X \times Y$ and T is a cycle of codimension i of X , then the action of correspondence has codimension $i + t - \dim(X)$ in Y . $t - \dim(X)$ is called the degree of the correspondence.

Equivalence relations are defined so that the above operations can be sensibly performed.

An equivalence relation on cycles of codimension i in a variety X for each i is called an adequate equivalence relation if

- Compatible with grading and addition. This can be defined by A cycle $C = \sum_i C_i$ where C_i is a cycle of codimension i is equivalent to zero cycle if and only if C_i is equivalent to zero cycle for each i , and if $C_1 \equiv 0$ and $C_2 \equiv 0$ then $C_1 + C_2 \equiv 0$. (and $-C_1 \equiv 0$)
- Compatibility with products: if Z is equivalent to 0 on X then $Z \times Y$ is equivalent to 0 in $Z(X \times Y)$.
- Compatibility with projections: If Z is equivalent to zero on $X \times Y$ then $(\text{pr}_X)_*(Z)$ is equivalent to zero.
- Moving Lemma: If Z and $W_1, \dots, W_l$ are cycles on X then there exists a cycle $Z' \equiv Z$ such that $Z' \cdot W_i$ is defined for $i = 1, \dots, l$

If an equivalence relation on cycles is adequate, then

- one can form the quotient groups on cycles modulo cycles equivalent to zero,

obtaining a ring with product induced from intersection of cycles.

- a morphism $f : X \rightarrow Y$ of smooth projective varieties over k induce homomorphisms f_* and f^* where f^* is a homomorphism of graded rings.
- A correspondence Z from X to Y of degree r induces a homomorphism from the equivalence classes of cycles of codimension i in X to equivalence classes of cycles of codimension $i + r$ of Y and equivalent correspondences induce the same map.

Rational, algebraic, homological and numerical equivalence are adequate equivalence relations.

Chow groups are cycles modulo rational equivalence. Note that rational equivalence can be seen as equivalent to equivalence by divisors of rational functions. (Fulton intersection theory describes the relation via using the map defining rational equivalence on $X \times \mathbf{P}^1$ as a rational function defined by the value of the map at two points, usually $[0 : 1]$ and $[1 : 0]$).

5.4. WEIL COHOMOLOGY

The main source for this section is [55] [53] [54].

There are various cohomology theories that deal with varieties over fields. If the field is of characteristic 0 then it is an extension of $\mathbb{Q}$ and if of transcendence degree 0 then it is a subfield of $\mathbb{C}$ with an embedding inside $\mathbb{C}$ (more generally an embedding into the algebraic closure of the field in question). Hence the variety can be seen as a complex analytic manifold, and deRham cohomology can be computed. There is also l -adic cohomology.

What is important about the cohomology functor is that it also acts on algebraic cycles under numerical equivalence in a way that is compatible with properties of any cohomological theory, such as Poincare Duality, and Künneth property, and other such relevant properties. Tannakian formalism is relevant in that sense. The basic properties required of a good cohomology theory are given below in the notion of a Weil cohomology theory.

A Weil Cohomology theory is a contravariant functor H from the category of smooth projective varieties over k into the graded vector spaces over a field F

satisfying:

- $H^i(X)$ is of finite dimension, and is zero for all i outside the range zero and twice the

dimension of X .

- Existence of cup product $\cup : H(X) \times H(X) \rightarrow H(X)$ that is graded, i.e. such that for $a \in H^i(X)$ and $b \in H^j(X)$ $a \cup b \in H^{i+j}(X)$ and “super-commutative” i.e. $b \cup a = (-1)^{ij} a \cup b$
- Poincaré duality there is a trace isomorphism $\text{tr} : H^{2d}(X) \xrightarrow{\sim} F$ such that

$$H^i(X) \times H^{2d-i}(X) \xrightarrow{\cup} H^{2d}(X) \xrightarrow{\text{tr}} F$$

is a perfect pairing, meaning that the map $H^i(X) \rightarrow \text{Hom}(H^{2d-i}(X), F)$ defined by the above map is an isomorphism.

- Künneth formula

$$H(X) \otimes H(Y) \xrightarrow{(\text{pr}_X)^* \otimes (\text{pr}_Y)^*} H(X \times Y)$$

is a graded isomorphism

- there are cycle class maps from Chow groups (of cycles under rational equivalence) to cohomology classes

$$\gamma_X : \text{CH}^i(X) \rightarrow H^{2i}(X)$$

which are

- functorial in the sense that for $f : X \rightarrow Y$ in the category of smooth projective schemes (or varieties) over k then $f^* \circ \gamma_Y = \gamma_X \circ f^*$ and $f_* \circ \gamma_X = \gamma_Y \circ f_*$
- multiplicativity $\gamma_{X \times Y}(Z \times W) = \gamma_X(Z) \otimes \gamma_Y(W)$
- compatible with intersection product by $\gamma_X(a \cdot b) = \gamma_X(a) \cup \gamma_X(b)$
- compatible with points P in the sense that $\text{Tr} \gamma_P = \iota \text{deg}$ or the commutative

$$\begin{array}{ccc} \text{CH}^0(P) & \xrightarrow{\gamma_P} & H^0(P) \\ \text{deg} \downarrow & & \downarrow \text{Tr} \\ \mathbb{Z} & \longrightarrow & F \end{array}$$

- Weak Lefschetz: if $i : Y \hookrightarrow X$ is a smooth hyperplane section, then $i^* : H^i(X) \rightarrow H^i(Y)$ is an isomorphism for $i < d - 1$ and injective for $i = d - 1$ where d is the dimension of X .

- Hard Lefschetz: Lefschetz operator $L(\alpha) = \alpha \cup \gamma_X(Y)$ induces isomorphisms $L^{d-i} : H^{d-i}(X) \rightarrow H^{d+i}(X)$ for $0 \leq i \leq d$

Examples of classical Weil cohomology theories are

- Betti-cohomology $H_B^i(X)$ which is the singular cohomology group $H^i(X_{\text{an}})$ where X_{an} is the complex manifold underlying X .
- classical de Rham cohomology $H_{dR}(X_{\text{an}})$
- algebraic de Rham $H^i(X_{\text{Zar}}, \Omega_{X/k})$
- étale cohomology $H_{\text{ét}}^i(X_{\bar{k}}, \mathbb{Q}_l)$ where $X_{\bar{k}} = X \otimes \bar{k}$ the variety considered over its algebraic closure, and l is a prime different than characteristic of k
- for k perfect, crystalline cohomology $H_{\text{crys}}(X/W(k)) \otimes K$ where K is the field of fractions of the Witt ring $W(k)$

5.5. MOTIVES

Definition 162 *Category of motives over a field k , denoted by M_k , is the category whose objects are triples (X, p, m) where X is a variety over k , $p \in C^{\dim(X)}(X \times X) = \text{Corr}^0(X, X)$ is a projector (i.e. $p^2 = p$) and m is an integer. The morphisms of the category are given by the following $\text{Hom}((X, p, m), (Y, q, n)) = qC^{\dim(X)-m+n}(X \times Y)p$*

(Note Kleiman defines morphisms in category of effective motives as equivalence classes satisfying $f \circ p = q \circ f$ modulo $f \circ p = q \circ f = 0$ where $f \in \text{Hom}((X, p), (Y, q))$, and does not introduce the grading, but mentions something similar later in the article [54].)

Note that $-\dim(X) \leq n-m \leq \dim(Y)$ for there to be a nonempty collection of morphisms.

The motivation for projector in defining the category of motives can be found in Deligne-Milne's Tannakian Categories, and Kleiman's motives.

The category of motives is an F -linear, pseudo-abelian category [54] Under product of varieties, it becomes a monoidal/tensorial/tannakian category.

In [48], the following result in [54] is quoted

Theorem 6 *M_k is an F -linear, pseudo-abelian category, cf. [K2] Sect. 5. Theorem 1.*

The main result of relevance in [48] is the following theorem.

Theorem 7 *The following properties are equivalent.*

- a) M_k is a semi-simple abelian category.
- b) $C^{\dim(X)}(X \times X)$ is a finite-dimensional, semi-simple F -algebra for every variety X .
- c) *The relation that motive correspondences should be seen as equivalent is numerical equivalence.*

5.6. MOTIVIC GALOIS GROUP

Main sources for what follows are [3] [86].

Let M_k denote the category of motives over k .

Proposition 10 *Betti realisation of cohomology functor $H_\sigma : M_k \rightarrow \text{Vect}_{\mathbf{Q}}$ based on an extension $\sigma : k \rightarrow \mathbb{C}$ is a fiber functor with values in $\mathbf{Q}$ -vector spaces. This is a faithful functor.*

(Here the role played by the embedding of the field inside $\mathbb{C}$ is not clear. Are the points of a scheme over k extended to a scheme over $\mathbb{C}$ in order to apply cohomology functor.)

Definition 163 *The scheme of automorphisms of the faithful cohomology functor, $\text{Aut}^\otimes(H_\sigma)$ is the motivic Galois group of k in the sense of Grothendieck. It will be denoted by G_{M_k} or MotGal_k . If one restricts the functor to all submotives (subvarieties) of a specific variety or a collection of varieties/motives W , one obtains the motivic Galois group of W , denoted by $G_{M_k(W)}$.*

5.6.1. What is known or assumed about the Motivic Galois Group

This is a proalgebraic group, equipped with a central homomorphism $w : G_m \rightarrow G_{\mathcal{M}(\mathcal{W})}$ and $\mathcal{M}(\mathcal{W})$ is graded, and functor $\mathcal{H}_B$ is a fibre functor which provides a tensor equivalence among categories $\mathcal{M}(\mathcal{W})$ and the category of rational representations of $G_{\mathcal{M}(\mathcal{W})}$ of finite dimension over $\mathbf{Q}$.

For all motives M of $\mathcal{M}(\mathcal{W})$ $G_{\mathcal{M}(\mathcal{W})}$ acts on $\mathcal{H}_B(M)$ through the algebraic group $G_{\mathcal{M}(M)}$

Furthermore

- $G_{\mathcal{M}(M)}$ is proreductive ($\mathcal{M}(\mathcal{W})$ is semisimple.)

- $G_{\mathcal{M}(M)}$ is the algebraic subgroup of $GL(\mathcal{H}_B(M))$ which fix motivated cycles among mixed tensors over $\mathcal{H}_B(M)$ reciprocally all mixed tensors over $\mathcal{H}_B(M)$ fixed by $G_{\mathcal{M}(M)}$ are motivated (this is defined earlier in article)
- $G_{\mathcal{M}(\mathcal{W})}$ unfolds over the composition of CM-fields, and the quotient of the center of $G_{\mathcal{M}(\mathcal{W})}$ by the image of w is compact by polarisability of $\mathcal{M}(\mathcal{W})$

5.6.2. Motivic Galois Group and Galois Group

Note that later in Serre's article "Propriétés Conjecturales ..." [86], there is a homomorphism from the Galois group to motivic Galois group which splits the exact sequence at least for $\mathbf{Q}_l$ on page 386 of [86].

Tying the information gathered here so far with Arthur's articles [6] and [7], at least when all algebraic groups are seen as over $\mathbf{Q}_l$ it seems possible to construct the map. Maybe it is possible to do everything over adeles or ideles in that case.

6. STANDARD CONJECTURES

6.1. STATEMENT OF STANDARD CONJECTURES

6.1.1. Grothendieck's Formulation

Direct quote from “Standard Conjectures on Algebraic Cycles” by A. Grothendieck [35].

- “The first is an existence assertion for algebraic cycles (considerably weaker than the Tate conjectures), and is inspired by and formally analogous to Lefschetz’s structure theorem on the cohomology of a smooth projective variety over the complex field.”
- “The second is a statement of positivity, generalising Weil’s well-known positivity theorem in the theory of abelian varieties. It is formally analogous to the famous Hodge inequalities, and is in fact a consequence of these in characteristic zero.”

6.1.2. Other formulations of the Conjectures by Grothendieck

Let k be an algebraically closed field of arbitrary characteristic. Let f be an endomorphism of a variety X/k . and $l \neq \text{char } k$ f induces $f^i \in \text{End}(H^i(X))$

Question 1 *Are the coefficients of the characteristic polynomials of f^i rational integers? Are they independent of l ? What if f is replaced by any cycle of dimension $\dim(X)$ in $X \times X$ considered as an algebraic correspondence?*

It is the case for characteristic zero using integral cohomology.

Let $\text{cl} : A^i(X) \otimes_{\mathbf{Z}} \mathbf{Q} \rightarrow H_l^{2i}(X)$ be the map which associates to each algebraic cycle its cohomology class. The image of this map is denoted by $C_l^i(X)$ the algebraic cohomology classes.

Lemma 63 (Dwork-Faton) *For integrality question it suffices to prove that*

$$\text{Tr } f_i^N \in \frac{1}{m} \mathbf{Z} \text{ for every } N \geq 0$$

where m is a fixed positive integer.

Let Γ_f denote the graph of f in $X \times X$ Let Δ denote the diagonal in $X \times X$. Let π_i be the projections of Δ onto $H^i(X) \otimes H^{n-i}(X)$ under the canonical decomposition of $H^n(X \times X)$

(where $n = \dim(X)$.)

Theorem 8 *If π are algebraic, then Dwork-Faton condition above holds.*

Proof 5 *A known calculation shows that*

$$\mathrm{Tr}(f^N)_{H^i} = (-1)^i \mathrm{cl}(\Gamma_{F^N}) \pi_i \in H^{4n}(X \times X) \cong \mathbf{Q}_l$$

If π_i are algebraic then $\pi_i = \frac{1}{m} \mathrm{cl}(\Pi_i)$ where Π_i is an algebraic cycle.

Conjecture 1 *Weak form of conjecture 1 ($C(X)$) The elements π_i^l (of the projection of the diagonal on the standard decomposition of the cohomology ring $H(X \times X)$) are algebraic (and come from an element of algebraic cycles of index i denoted by $A^i(X) \otimes_{\mathbf{Z}} \mathbf{Q}$ which is independent of l)*

Note1 statement in parenthesis for establishing independence of P_i (I am assuming that this refers to the polynomials appearing in zeta function of the variety) on l . Note2 If $C(X)$ and $C(Y)$ hold then $C(X \times Y)$ holds. More generally Künneth components of any algebraic cohomology class on $X \times Y$ are algebraic.

Let X be smooth and projective. Let $\xi \in H^2(X)$ be the class of a hyperplane section. Let

$$\cup \xi^{n-i} : H^i(X) \rightarrow H^{2n-i}(X) \ (i \leq n).$$

Known result this is an isomorphism over the complex field by transcendental methods due to Lefschetz. The hard Lefschetz theorem is proved in [32] page 122.

For $i = 2j$ there is a commutative square:

$$\begin{array}{ccc} H^{2j}(X) & \xrightarrow{\cup \xi^{n-2j}} & H^{2n-2j}(X) \\ \uparrow & & \uparrow \\ C^j(X) & \rightarrow & C^{n-j}(X) \end{array}$$

Question 2 *Is this an isomorphism for all characteristics?*

Conjecture 2 ($A(X)$):

(a) $\cup \xi^{n-i}$ is always an isomorphism.

(b) if $i = 2j$ then the above induces an isomorphism (or equivalently an epimorphism) for algebraic cohomology classes $C^j(X) \rightarrow C^{n-j}$

Note1 If $C^j(X)$ is assumed to be finite dimensional, (b) is equivalent to the assertion that $\dim C^{n-j} \leq \dim C^j(X)$ (which in particular implies the equality of these dimensions in view of (a)).

An equivalent formulation of the above for all varieties X as above is

Conjecture 3 ($B(X)$) The Λ -operation (see A Weil Variétés Kähleriennes [98]) of Hodge theory is algebraic.

This means that there is an algebraic cohomology class λ in $H^*(X \times X)$ such that the map $\Lambda : H^*(X) \rightarrow H^*(X)$ is got by lifting a class from X to $X \times X$ by the first projection, cupping with λ and taking the image in $H^*(X)$ by the Gysin homomorphism associated to the second projection.

Theorem 9 • $B(X) \Rightarrow A(X)$

- $A(X \times X) \Rightarrow B(X)$
- $B(X) \Rightarrow C(X)$ (first part)

Conjecture 4 Conjecture 2 of Hodge type ($\text{Hdg}(X)$) Let $P^i(X)$ be the primitive part of $H^i(X)$ i.e. $\ker(\cup \xi^{n-i+1})$. Let $C_{\text{Pr}}^j = P^{2j} \cap C^j(X)$. The symmetric bilinear form on C_{Pr}^j defined by

$$(x, y) \mapsto (-1)^j K(x \cdot y \cdot \xi^{n-2j})$$

where K stands for the isomorphism $H^{2n}(X) \cong \mathbf{Q}_l$ is positive definite.

Remark1 One is easily reduced to the case when $\dim(X) = 2m$ is even, and $j = m$.

Theorem 10 (1) ($\text{Hdg}(X)$) holds for characteristic zero.

(2) $B(X)$ and $\text{Hdg}(X \times X)$ imply (Weil, Serre) if $f \in \text{End}(X)$ such that $f^*(\xi) = q\xi$ for some $q \in \mathbf{Q}$ which is necessarily positive, then the eigenvalues of $f_{H^i(X)}$ are algebraic integers of absolute value $q^{i/2}$ i.e. Weil conjectures follow.

- (3) $\text{Hdg}(X)$ and $A(X)$ (a) (Lefschetz conjecture in cohomology) implies that numerical equivalence of cycles is the same as cohomological equivalence for any l -adic cohomology if and only if $A(X)$ holds.
- (3b) in characteristic zero, $A(X)$ is equivalent to the equality of cohomological and numerical equivalence.
- (4) $B(X)$ and $\text{Hdg}(X)$ imply that numerical equivalence of cycles coincides with $\mathbf{Q}_l$ -equivalence for any l .
- (4b) The natural map

$$Z^i(X) \otimes_{\mathbf{Z}} \mathbf{Q}_l \rightarrow H_l^i(X)$$

is a monomorphism and in particular

$$\dim_{\mathbf{Q}} C^i(X) \leq \dim_{\mathbf{Q}_l} H_l^i(X)$$

(nondegeneracy suffices for this deduction)

- (4c) Another consequence of $\text{Hdg}(X)$ and $B(X)$ is the stronger version of $B(X)$ that Λ comes from an algebraic cycle with rational coefficients independent of l

6.1.3. Steven Kleiman's Restatement

6.2. RATIONALE

Grothendieck's rationale for making the statement of standard conjectures is for proving Weil conjectures when approached through l -adic cohomology. The $Z-(\zeta-)$ function can be expressed in terms of polynomials that involve cohomological expressions. To be more precise we are on a variety over a field of finite characteristic, and we are dealing with l -adic cohomology group of the variety over the algebraic closure of the base field of finite characteristic, and also characteristic polynomial of the action of the Frobenius endomorphism on cohomology groups.

Let $P_i(t) = t^{\dim H^i(\bar{X})} Q_i(t^{-1})$, where Q_i is the characteristic polynomial of the action of the Frobenius endomorphism of X on $H^i(\bar{X})$, and cohomology is l -adic cohomology and $\bar{X}$ is deduced from X by base extension to the algebraic closure of F_q . The first conjecture would prove the part of Weil conjectures about polynomial $P_i(t)$ having integral coefficients

independent of $l \neq \text{char} F$. The first and second conjecture would prove eigenvalues of Frobenius endomorphism of the cohomology group are of absolute value $q^{i/2}$ where q is the base field size, and i is the grading of the cohomology group. Here Grothendieck makes a reference to Serre's article [80].

6.2.1. Summary of Serre's Article

The main theorems in the article "Analogues Kählériens de Certaines Conjectures de Weil" [80] are quoted below:

Theorem 11 *Let V be a projective irreducible nonsingular variety defined over the field $\mathbb{C}$ of complex numbers. Let $f : V \rightarrow V$ be a morphism of V into itself. Suppose that there is an integer $q > 0$ and a hyperplane section E of V such that the divisor $f^{-1}(E)$ is algebraically equivalent to $q \cdot E$. Then for all integers $r \geq 0$ the proper values of the endomorphism f_r^* of $H^r(V, \mathbb{C})$ defined by f have absolute value $q^{r/2}$.*

Note that if $\mathbb{C}$ is replaced by a finite field $\mathbb{F}_q$ and f by the corresponding Frobenius morphism, the divisor $f^{-1}(E)$ is equivalent to $q \cdot E$ and theorem 1 is the kählerian analogue of Riemann's hypothesis.

I am not quoting the second theorem just yet as this has preliminary definitions.

But basically there is a discussion on differential forms and cohomology classes of complex varieties with a review of "varietes kahleriennes" by A Weil, an algebraic function g defined from f^* which is an endomorphism of the cohomology ring a cohomology class u (in second cohomology) of kählerian type, which later (via the cohomology ring product which is cup product) defines an endomorphism L_V of the cohomology ring (shifting grading by two). and a nondegenerate positive Hermitian form $T_V(a, b)$

These objects have certain relations which leads to kählerian analogue of functional equation of the zeta function. I am omitting details just this moment because they entail covering kähler varieties.

Then there are cohomological correspondences (in grading (n, n)) in product of two varieties, and a condition of compatibility of such a correspondence with kählerian structure

of V and W given by

$$X \text{ maps } L_V^r(\text{Ker} L_V^s) \text{ within } L_W^r(\text{Ker} L_W^s)$$

for all integers $r, s \geq 0$ Remark in the algebraic case, one should speak of polarizations.

Here a correspondence is defined in this article as below.

Definition 164 *Let V and W be two compact and connected kählerian varieties of dimension n . A correspondence X of V in W is a $\mathbb{C}$ -linear map $H(V) \rightarrow H(W)$ which preserves the bidegrees, and commutes with conjugation (in other words a real operator) such that X corresponds to a real cohomology class of type (n, n) in $V \times W$.*

For all integers r with $0 \leq r \leq 2n$ one may define a linear transformation

$$X'_r : H^r(W, \mathbb{C}) \rightarrow H^r(V, \mathbb{C})$$

by the formula

$$X'_r = L_V^{r-n} \circ {}^t X_{2n-r} \circ L_V^{n-r}.$$

where ${}^t X : H(W) \rightarrow H(V)$ is the transpose of X via Poincare duality, Hodge decomposition being self-dual, and ${}^t X$ verifying compatibility condition (of a correspondence with a kählerian structure listed above.

X'_r plays the role of ξ' in Castelnuovo's formula.

Theorem 12 *Let V and W be two connected kählerian varieties of same dimension and X a correspondence compatible with kählerian structures of V and W . For all integers r ,*

$$\text{Tr}(X_r \circ X'_r) \geq 0$$

and if $\text{Tr}(X_r \circ X'_r) = 0$ then $X_r = 0$.

Note that by considering the Hermitian forms $T_V(.,.)$ and $T_W(.,.)$ a simple calculation where compatibility condition plays an essential role shows that the operators X_r and X'_r are adjoint under these forms. The trace of $X_r \circ X'_r$ is nothing else than the norm square (in the sense of Hilbert-Schmidt) of the operator X_r and so theorem is evident.

Then there is some more statements (of fair importance) that I am skipping for now.

6.2.2. Weil Conjectures

Let $X/\mathbb{F}_q$ be a smooth irreducible variety of dimension n over the finite field $\mathbb{F}_q$ with q elements, and $l \neq \text{char}(\mathbb{F}_q)$ a prime.

The ζ -function of X can be expressed as (proof by Artin and Grothendieck)

$$\zeta_X(t) = \frac{L'(t)}{L(t)}$$

$$L(t) = \frac{L_0(t)L_2(t) \dots L_{2n}(t)}{L_1(t)L_3(t) \dots L_{2n-1}(t)}$$

$$L_i(t) = \frac{1}{P_i(t)}$$

$$P_i(t) = t^{\dim H^i(\bar{X})} Q_i(t^{-1})$$

where Q_i is the characteristic polynomial of the action of the Frobenius endomorphism of X on $H^i(\bar{X})$. and here cohomology is l -adic cohomology group, and $\bar{X}$ is obtained from X by extension to algebraic closure of $\mathbb{F}_q$.

Conjecture 5 Weil conjectures

- (a) the $P_i(t) \in \mathbb{Z}[t]$ independent of $l \neq \text{char} \mathbb{F}$
- (b) the eigenvalues of the Frobenius endomorphism on $H^i(\bar{X})$ i.e. reciprocals of the roots of $P_i(t)$ are of absolute value $q^{i/2}$.

Remark, Hartshorne's Algebraic Geometry has an appendix on Weil Conjectures, and the cohomological interpretation of the proof of Weil conjectures is sketched there. For a thorough exposition, need to have some understanding of étale cohomology through which l -adic cohomology is defined.

7. WEIL GROUP AND ALGEBRAIC NUMBER THEORY

The main source for this section is [94].

7.1. PRELIMINARIES

7.1.1. Weil Group's Definition in Tate's Number Theoretic Background (NTB)

For a topological group G , $G^c = \overline{[G, G]}$ is the closure of the commutator subgroup, and $G^{\text{ab}} = G/G^c$. If H is a closed subgroup of G of finite index, there is a transfer homomorphism $t : G^{\text{ab}} \rightarrow H^{\text{ab}}$. For a section $s : G/H \rightarrow G$, transfer homomorphism is defined by $t(g) = \pi^{\text{ab}} \prod_{x \in G/H} s(x)gs(xg)^{-1}$ where $\pi^{\text{ab}} : H \rightarrow H^{\text{ab}}$ is the abelianization map.

Definition of Weil group. Let F be a local or global field and $\bar{F}$ a separable algebraic closure of F . For each such finite extension E of F in $\bar{F}$, let $G_E = \text{Gal}(\bar{F}/E)$.

A Weil group for $\bar{F}/F$ is not really just a group but a triple (W_F, φ, r_E) . Here

- W_F is a topological group.
- $\varphi : W_F \rightarrow G_F$ is a continuous homomorphism with dense image.
- $r_E : C_E \rightarrow W_E^{\text{ab}}$ is an isomorphism of topological groups, where

$$- G_E = \text{Gal}(\bar{F}/E)$$

$$- W_E = \varphi^{-1}(G_E)$$

$$- C_E = \begin{cases} \text{Multiplicative group } E^* & F \text{ is a local field} \\ \text{idele class group } \mathbf{A}_E^*/E^* & F \text{ is a global field} \end{cases}$$

Remark The continuity of φ just means that W_E is open in W_F for each E , (as G_E are the basic open sets in G_F) and its having dense image means that φ induces a bijection of homogeneous spaces:

$$\tilde{\varphi} : W_F/W_E \rightarrow G_F/G_E \cong \text{Hom}_F(E, \bar{F})$$

for each E , and in particular, a group isomorphism $W_F/W_E \cong \text{Gal}(E/F)$ when E/F is Galois.

Weil group must satisfy the following four conditions:

(W1) For each E , the composed map $\varphi^{\text{ab}} \circ r_E$ is the Artin reciprocity map (law) of class field theory. i.e.

$$C_E \xrightarrow{r_E} W_E^{\text{ab}} \xrightarrow{\varphi^{\text{ab}}} G_E^{\text{ab}}$$

(W2) For $w \in W_F$ and $\sigma = \varphi(w) \in G_F$, and for each E the following diagram commutes:

$$\begin{array}{ccc} C_E & \xrightarrow{r_E} & W_E^{\text{ab}} \\ \downarrow \sigma & & \downarrow c_w \\ C_{E^\sigma} & \xrightarrow{r_{E^\sigma}} & W_{E^\sigma}^{\text{ab}} \end{array}$$

where c_w is conjugation by w , and $\sigma \in G_F$ induces a map $C_E \rightarrow C_{E^\sigma}$, denoted by the same letter.

(W3) For $E' \subset E$, the following diagram commutes

$$\begin{array}{ccc} C_{E'} & \xrightarrow{r_{E'}} & W_{E'}^{\text{ab}} \\ \downarrow \iota & & \downarrow \text{transfer} \\ C_E & \xrightarrow{r_E} & W_E^{\text{ab}} \end{array}$$

(W4) The natural map

$$W_F \rightarrow \varprojlim_E W_{E/F}$$

is an isomorphism of topological groups, where $W_{E/F} = W_F/W_E^c$, and projective limit is ordered by inclusion $E \rightarrow \bar{F}$.

Lemma 64 *If W_F is a Weil group for $\bar{F}/F$, then for each finite extension E of F in $\bar{F}$, W_E (furnished with the restriction of φ and the isomorphisms $r_{E'}$ for $E' \supset E$) is a Weil group for $\bar{F}/E$.*

Lemma 65 *For $F \subset E' \subset E \subset \bar{F}$, we have the commutative diagram:*

$$\begin{array}{ccc} W_{E'}/W_E & \longrightarrow & G_{E'}/G_E \\ \downarrow & & \downarrow \\ W_F/W_E & \longrightarrow & G_F/G_E \\ \downarrow & & \downarrow \\ W_F/W_{E'} & \longrightarrow & G_F/G_{E'} \end{array}$$

Lemma 66 (W5) *If W_F is a Weil group, then for each $F \subset E' \subset E$ the diagram*

$$\begin{array}{ccc} C_E & \xrightarrow{r_E} & W_E^{\text{ab}} \\ N_{E/E'} \downarrow & & \downarrow \tilde{\iota} \\ C_{E'} & \xrightarrow{r_{E'}} & W_{E'}^{\text{ab}} \end{array}$$

is commutative, where $\tilde{\iota} : W_E^{\text{ab}} \rightarrow W_{E'}^{\text{ab}}$ is induced by inclusion $\iota : E' \rightarrow E$, and hence $G_E \rightarrow G_{E'}$ and $W_E \rightarrow W_{E'}$

Note that the norm map is the product of all the Galois conjugates, and by (W2), Galois group action corresponds to conjugation by the corresponding Weil group element. On the other hand, the composition of $\tilde{\iota}$ with transfer map in (W3), gives the product of all the conjugates. Therefore we have the commutative diagram

$$\begin{array}{ccc} C_E & \xrightarrow{r_E} & W_E^{\text{ab}} \\ N_{E/E'} \downarrow & & \downarrow \tilde{\iota} \\ C_{E'} & & W_{E'}^{\text{ab}} \\ \iota \downarrow & & \downarrow \text{transfer} \\ C_E & \xrightarrow{r_E} & W_{E'}^{\text{ab}} \end{array}$$

Therefore:

$$\text{tr} \circ \tilde{\iota} \circ r_E = \text{tr} \circ r_{E'} \circ N_{E/E'}$$

If we can argue that $\iota : C_{E'} \rightarrow C_E$ being induced by the inclusion $E' \rightarrow E$ is injective, implies, transfer map here being injective, then we are done.

In fact, (W3), and injectiveness of ι enforce, transfer map being injective.

Remark W_E^{ab} is a subgroup of $W_{E/F}$ and if $\sigma \in G_F$ carries E to E^σ then in $W_{E/F}$, W_E^{ab} and $W_{E^\sigma}^{\text{ab}}$ are conjugate, as stated in (W2).

7.1.2. Construction of Weil group, Tate - NTB

Lemma 67 *Let W_F be a Weil group for $\bar{F}/F$. Then for each Galois E/F the group $W_{E/F} = W_F/W_E^c$ is an extension of $W_F/W_E = \text{Gal}(E/F)$ by $W_E^{\text{ab}} = W_E/W_E^c \cong C_E$.*

Note that we have the exact sequence:

$$(W6) \begin{array}{ccccccc} 1 & \longrightarrow & W_E/W_E^c & \longrightarrow & W_F/W_E^c & \longrightarrow & W_F/W_E \longrightarrow 1 \\ & & \downarrow r_E^{-1} & & \downarrow \text{id} & & \downarrow \tilde{\varphi} \\ 1 & \longrightarrow & C_E & \longrightarrow & W_{E/F} & \longrightarrow & \text{Gal}(E/F) \longrightarrow 1 \end{array}$$

In fact F above may be replaced with E' where $F \subseteq E' \subseteq E \subseteq \bar{F}$.

Lemma 68 *If $\alpha_{E/F} \in H^2(\text{Gal}(E/F), C_E)$ denotes the class of the group extension above, then for each $n \in \mathbb{Z}$, $\alpha_{E/F}$ induces maps by taking cup-product in cohomology:*

$$H^n(\text{Gal}(E/F), \mathbb{Z}) \rightarrow H^{n+2}(\text{Gal}(E/F), C_E).$$

Furthermore, this is an isomorphism.

Rationale: $C_{E'} \rightarrow C_E^{\text{Gal}(E/E')}$ is a bijection for $F \subset E' \subset E$. (W3) and abstract cohomological theorem implies that this is an isomorphism.

The following theorem and its corollary are quoted from Class Field Theory notes by Artin and Tate [93, p 184].

Theorem 13 *Let $U/A \cong G$ be a group extension belonging to the class $\alpha \in H^2(G, A)$. Then the following diagram is commutative:*

$$\begin{array}{ccccccc} 0 & \longrightarrow & A/(U^c \cap A) & \xrightarrow{\bar{i}} & U/U^c & \xrightarrow{\bar{j}} & G/G^c \cong H^{-2}(G, \mathbb{Z}) \longrightarrow 0 \\ & & \downarrow \bar{N} & & \downarrow V_{U,A} & & \downarrow \alpha \\ 0 & \longrightarrow & NA & \xrightarrow{\text{incl.}} & A^G & \xrightarrow{\mathcal{H}} & H^0(G, A) \longrightarrow 0 \end{array}$$

where the right-hand vertical arrow denotes multiplication by α , and $\bar{N}$, $\bar{i}$, and $\bar{j}$ denote the maps induced in the obvious way by $N : A \rightarrow NA$, and by $A \xrightarrow{i} U \xrightarrow{j} G$.

(Remark: Norm map $N : A \rightarrow A$, is defined by $Na = \prod_{\sigma \in G} a^\sigma$. $V_{U,A} : U/U^c \rightarrow A/A^c = A$, is the transfer map. A is abelian and a G -module, G a finite group.)

Corollary 3 *Let $U/A \cong G$ be a group extension belonging to the class $\alpha \in H^2(G, A)$. Consider the following three homomorphisms:*

- $V : U/U^c \rightarrow A^G$

- $\alpha_{-3} : H^{-3}(G, \mathbb{Z}) \rightarrow H^{-1}(G, A)$
- $\alpha_{-2} : H^{-2}(G, \mathbb{Z}) \rightarrow H^0(G, A)$

There exist exact sequences

$$0 \longrightarrow H^{-1}(G, A)/\text{Im}\alpha_{-3} \longrightarrow \text{Ker}V \longrightarrow \text{Ker}\alpha_{-2} \longrightarrow 0$$

and

$$0 \longrightarrow A^G/\text{Im}V \longrightarrow H^0(G, A)/\text{Im}\alpha_{-2} \longrightarrow 0$$

In particular V is an isomorphism into if and only if α_{-3} is onto and α_{-2} is an isomorphism into; V is onto if and only if α_{-2} is onto.

The following theorem is quoted from Serre's Corps Locaux p 154. In section “comparison theorem”, Theorem 12, p. 154, of [81].

Theorem 14 *Let G be a finite group, and A, A' two G -modules and $f : A' \rightarrow A$ a G -homomorphism. For all primes p let G_p be a p -Sylow subgroup of G . Suppose there exists an integer n_p such that the homomorphism*

$$f_i^* : \hat{H}^i(G_p, A') \rightarrow \hat{H}^i(G_p, A)$$

is surjective for $i = n_p$ bijective for $i = n_p + 1$ and injective for $i = n_p + 2$. If B is a G -module such that $\text{Tor}(A, B) = \text{Tor}(A', B) = 0$ then the homomorphism

$$\hat{H}^i(g, A' \otimes B) \rightarrow \hat{H}^i(g, A \otimes B)$$

is bijective for all subgroups g of G and for all $i \in \mathbb{Z}$. In particular $\hat{H}^i(g, A') \rightarrow \hat{H}^i(g, A)$ is bijective for all i .

In fact, the next section in Local Fields [81] is “The theorem of Tate and Nakayama”, which allows us to conclude that taking cup product with α induces an isomorphism, under the conditions stated in the theorem, and a generalization.

Remark Negative cohomology groups are defined (except for $i = -1$) via homology groups. Homology groups are defined on p 122 in Serre's Corps Locaux [81]. For a G -module A , $A_G = A/\langle s \cdot a - a | a \in A, s \in G \rangle$ The functor A_G is additive and right-

exact. Its left derived functors are the homology groups. i.e. $H_0(G, A) = A_G = \mathbb{Z} \otimes_{\Lambda} A$ and $H_q(G, A) = \text{Tor}_q^{\Lambda}(\mathbb{Z}, A)$. If $\{P_i\}$ is a projective resolution of $\mathbb{Z}$, then the homology groups are the homology groups of the chain complex formed by $P_i \otimes_{\Lambda} A$. Here $B \otimes_{\Lambda} A$, B is a right Λ -module by $bs = s^{-1}b$. If $N : A \rightarrow A$, is defined by $Na = \sum_{s \in G} sa$, and I_G is the augmentation ideal of $\mathbb{Z}[G]$, defined by $I_G = \langle s - 1 \mid s \in G \rangle$, and $A^G = \{a \in A \mid sa = a \forall s \in G\}$. then

$$I_G A \subset \text{Ker}(N), \text{Im}(N) \subset A^G$$

and

$$H_0(G, A) = A/I_G A, H^0(G, A) = A^G.$$

By passing to the quotient N induces a homomorphism

$$N^* : H_0(G, A) \rightarrow H^0(G, A)$$

and one defines:

$$\hat{H}_0(G, A) = \text{Ker}(N^*) \hat{H}^0(G, A) = \text{Coker}(N^*)$$

By letting ${}_N A$ be the kernel of N operating on A , we have

$$\hat{H}_0(G, A) = {}_N A/I_G A \hat{H}^0(G, A) = A^G/{}_N A$$

Then one defines

$$\hat{H}^n(G, A) = H^n(G, A) \text{ for } n \geq 1$$

$$\hat{H}^0(G, A) = A^G/{}_N A$$

$$\hat{H}^{-1}(G, A) = {}_N A/I_G A$$

$$\hat{H}^{-n}(G, A) = H_{n-1}(G, A) \text{ for } n \geq 2.$$

Lemma 69 *The canonical classes are related by:*

$$\text{infl}_{\alpha_{E'/F}} = [E : E']\alpha_{E/F} \text{ and } \text{res}_{\alpha_{E/F}} = \alpha_{E/E'}$$

For the first, use Theorem 6 on p. 188 Artin-Tate Class Field Theory [93]; the second is obvious.

Theorem 15 *For $\alpha \in H^2(G, A)$ we have*

$$\text{infl}_{(G/H), G^v G, (G/H)} \alpha = \alpha^{(H:1)}$$

7.1.3. Consequences of the Canonical Class Isomorphism

Applying the result that taking cup-product with the canonical class gives isomorphism on cohomology groups, with $n = -1, 0, -2$, assuming $G = \text{Gal}(E/F)$ acts trivially on $\mathbb{Z}$.

- $n = -1$ we obtain the isomorphism $\alpha_{-1}(E/F) : H^{-1}(\text{Gal}(E/F), \mathbb{Z}) \rightarrow H^1(\text{Gal}(E/F), C_E)$. But $H^{-1}(\text{Gal}(E/F), \mathbb{Z}) \cong {}_N\mathbb{Z}/I_G\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = 0$.
- $n = 0$, we obtain the isomorphism $\alpha_0(E/F) : H^0(\text{Gal}(E/F), \mathbb{Z}) \rightarrow H^2(\text{Gal}(E/F), C_E)$. But $H^0(\text{Gal}(E/F), \mathbb{Z}) \cong \mathbb{Z}^G/N\mathbb{Z} = \mathbb{Z}/|G|\mathbb{Z}$ is cyclic of order $|G| = |\text{Gal}(E/F)| = [E : F]$. It is generated by $\alpha_{E/F}$.
- $n = -2$, we obtain the isomorphism $\alpha_{-2}(E/F) : H^{-2}(\text{Gal}(E/F), \mathbb{Z}) \rightarrow H^0(\text{Gal}(E/F), C_E)$. But $H^{-2}(\text{Gal}(E/F), \mathbb{Z}) = H_1(\text{Gal}(E/F), \mathbb{Z}) = G_{E/F}^{\text{ab}}$ and $H^0(\text{Gal}(E/F), C_E) = C_E^G/NC_E = C_F/N_{E/F}C_E$. The isomorphism is the Artin reciprocity map.

Lemma 70 $H^1(G, \mathbb{Z}) \cong G^{\text{ab}}$

Neukirch “Cohomology of Number Fields”: Let $A^* = \text{Hom}(A, \mathbb{Q}/\mathbb{Z})$, we have a natural isomorphism

$$H^i(G, A^*) \cong H_i(G, A)^*$$

for $i \geq 0$.

Also we have

$$H^2(G, \mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) = \text{Hom}_{\text{cts}}(G, \mathbb{Q}/\mathbb{Z}) = (G^{\text{ab}})^{\vee}$$

where $X^{\vee} = \text{Hom}_{\text{cts}}(A, \mathbb{R}/\mathbb{Z})$ is the Pontryagin dual.

If A is topologically finitely generated, then $A^{\vee} \cong A^*$, also the case if A is finite or discrete torsion.

Then we have

$$H_1(G, \mathbb{Z})^* \cong H^1(G, \mathbb{Z}^*) = H^1(G, \mathbb{Q}/\mathbb{Z}) = (G^{\text{ab}})^*$$

Therefore $H_1(G, \mathbb{Z}) = G^{\text{ab}}$.

Lemma 71 $W_{E/F}^{\text{ab}} = W_F^{\text{ab}}$.

Note $W_{E/F} = W_F/W_E^c$, and

$$W_{E/F}^{\text{ab}} = (W_F/W_E^c)/(W_F/W_E^c)^c = (W_F/W_E^c)/(W_F^c/W_E^c) = W_F/W_F^c = W_F^{\text{ab}}.$$

The only worrisome step, is the second one. If one can be convinced that $(W_F/W_E^c)^c = W_F^c/W_E^c$, then the rest is trivial. In general note, if $B \leq A$, and B is normal in A , and $x, y \in A$, then $[xB, yB] = [x, y]B$. And most certainly $[B, B] \leq [A, A] \cap B$.

Lemma 72 *The isomorphism $C_F/N_{E/F}C_E \cong \text{Gal}(E/F)^{\text{ab}}$ is Artin reciprocity, and coincides with taking cup product with fundamental class.*

Using previous lemma, and computing the cokernels of the vertical maps, we obtain the following commutative diagram:

$$\begin{array}{ccccc} C_E & \longrightarrow & W_E^{\text{ab}} & \longrightarrow & G_E^{\text{ab}} \\ \downarrow N_{E/F} & & \downarrow \tilde{\iota} & & \downarrow \\ C_F & \longrightarrow & W_F^{\text{ab}} & \longrightarrow & G_F^{\text{ab}} \\ \downarrow & & \downarrow & & \downarrow \\ C_F/N_{E/F}C_E & \longrightarrow & (W_F/W_E)^{\text{ab}} & \longrightarrow & \text{Gal}(E/F)^{\text{ab}} \end{array}$$

Note that the diagonal maps

$$\begin{array}{ccccc}
 C_E & \longrightarrow & W_E^{\text{ab}} & \longrightarrow & G_E^{\text{ab}} \\
 \downarrow N_{E/F} & \searrow & \downarrow \tilde{\iota} & & \downarrow \\
 C_F & \longrightarrow & W_F^{\text{ab}} & \longrightarrow & G_F^{\text{ab}} \\
 \downarrow & & \downarrow & \searrow & \downarrow \\
 C_F/N_{E/F}C_E & \longrightarrow & (W_F/W_E)^{\text{ab}} & \longrightarrow & \text{Gal}(E/F)^{\text{ab}}
 \end{array}$$

arise from the abelianization of the exact sequence

$$\begin{array}{ccccccc}
 1 & \longrightarrow & W_E/W_E^c & \longrightarrow & W_F/W_E^c & \longrightarrow & W_F/W_E \longrightarrow 1 \\
 & & \downarrow r_E^{-1} & & \downarrow \text{id} & & \downarrow \tilde{\varphi} \\
 1 & \longrightarrow & C_E & \longrightarrow & W_{E/F} & \longrightarrow & \text{Gal}(E/F) \longrightarrow 1 \\
 & & \downarrow & & \downarrow \text{ab} & & \downarrow \text{ab} \\
 & & C_E & \longrightarrow & W_F^{\text{ab}} & \longrightarrow & \text{Gal}(E/F)^{\text{ab}}
 \end{array}$$

Remark There may be problems with the argument above, in particular the last statement. It seems to be true, since everything is induced from the maps φ and r_E , but that abelianization and norm should have an interplay may need proof.

Considering cyclic extensions: For E/F cyclic, the isomorphism

$$C_F/N_{E/F}C_E \cong \text{Gal}(E/F)^{\text{ab}}$$

determines $\alpha_{E/F}$ and it follows that $\alpha_{E/F}$ is the “canonical” or “fundamental” class of class field theory.

Extending to general case: The same is true for arbitrary E/F as one sees by taking a cyclic E_1/F of the same degree as E/F , and inflating $\alpha_{E_1/F}$ and $\alpha_{E/F}$ to EE_1/F , where they are equal by $\text{infl}\alpha_{E'/F} = [E : E']\alpha_{E/F}$, with $E = EE_1$ and $E' = E, E_1$.

Conclusion of existence argument Conversely, if we are given classes $\alpha_{E/E'}$ satisfying the conditions for inflation and restriction and such that the maps on cohomology by taking cup product with $\alpha_{E/F}$ are isomorphisms, then we can construct a Weil group W_F as the projective limit of group extensions $W_{E/F}$ made with these classes.

This construction is abstracted and carried out in great detail in Chapter XIV of [93]. The existence of such classes $\alpha_{E/E'}$ is proved in [93] and [18].

7.1.4. Uniqueness of Weil Group

A Weil group is unique up to isomorphism.

Proposition 11 *Let W_F and W'_F be two Weil groups for $\bar{F}/F$. There exists an isomorphism $\theta : W_F \rightarrow W'_F$ such that the diagrams*

$$\begin{array}{ccc}
 & W_E^{\text{ab}} & \\
 r_E \nearrow & \downarrow \theta^{\text{ab}} & \\
 C_E & & W_E'^{\text{ab}} \\
 r_E' \searrow & & \\
 & &
 \end{array}
 \quad \text{and} \quad
 \begin{array}{ccc}
 W_F & \xrightarrow{\varphi} & \text{Gal}(\bar{F}/F) \\
 \theta \downarrow & & \uparrow \varphi' \\
 W'_F & &
 \end{array}$$

are commutative.

For each finite Galois E/F , let $I(E)$ denote the set of isomorphisms θ such that the following diagram is commutative:

$$\begin{array}{ccccccc}
 1 & \longrightarrow & C_E & \longrightarrow & W_{E/F} & \longrightarrow & \text{Gal}(E/F) \longrightarrow 1 \\
 & & \downarrow \text{id} & & \downarrow \tilde{\theta} & & \downarrow \text{id} \\
 1 & \longrightarrow & C_E & \longrightarrow & W'_{E/F} & \longrightarrow & \text{Gal}(E/F) \longrightarrow 1
 \end{array}$$

Since the two group extensions $W_{E/F}$ and $W'_{E/F}$ each have the same class, namely the canonical class $\alpha_{E/F}$ as their cohomology class, $I(E)$ is not empty.

Since $H^1(\text{Gal}(E/F), C_E) = 0$, an isomorphism in $I(E)$ is determined up to composing with an inner automorphism of $W_{E/F}$ by an element of $C_E \cong W_E^{\text{ab}}$.

The center of $W_{E/F}$ is C_E , and C_E/C_F is compact. Hence $I(E)$, as principal homogeneous space for C_E/C_F , has a natural compact topology.

For $E_1 \supset E$, the natural map $I(E_1) \rightarrow I(E)$ is continuous for this topology, since it is reflected in the norm map $N_{E_1/E}$ once we pick an element of $I(E_1)$.

Hence the projective limit $\varprojlim I(E)$ is not empty.

An element θ of this limit gives an isomorphism $W_E \rightarrow W'_E$; by (W4), and has the required properties.

It turns out (cf. (1.5.2)) that θ is unique up to an inner automorphism of W_F by an element $w \in \text{Ker}\varphi$.

7.1.5. Special Cases

This subsection a quote from NTB.

In local nonarchimedean and global function field case, G_F is a completion of W_F .

In local archimedean and number field case, G_F is a quotient of W_F .

Local Nonarchimedean

For each E , let k_E be the residue field of E and $q_E = \text{Card}(k_E)$. Let $\bar{k} = \cup_E k_E$. We can take W_F to be the dense subgroup of G_F consisting of the elements $\sigma \in G_F$ which induce on $\bar{k}$ the map $x \mapsto x^{(q_F^n)}$ for some $n \in \mathbb{Z}$. This W_F contains the inertia group I_F (the subgroup of G_F fixing $\bar{k}$), and $W_F/I_F \approx \mathbb{Z}$. The topology in W_F is that for which I_F gets the profinite topology induced from G_F and is open in W_F . The map $\varphi : W_F \rightarrow G_F$ is inclusion, and the maps $r_E : E^* \rightarrow W_E^{\text{ab}}$ are the reciprocity law homomorphisms. Concerning the sign of the reciprocity law, our convention will be that $r_E(a)$ acts as $x \mapsto x^{|a|_E}$ on $\bar{k}$, where $|a|_E$ is the normed absolute value of an element $a \in E^*$. If π_E is a uniformizer in E , then $|\pi_E|_E = q_E^{-1}$; thus our convention is that uniformizers correspond to the inverse of the Frobenius automorphism.

Global Nonarchimedean - Function Field

This is same as above, residue field is to be replaced with constant field, inertia group with geometric Galois group $\text{Gal}(\bar{F}/F\bar{k})$, define the norm $|a|_E$ of an idele class $a \in C_E$ to be the product of the normed absolute values of the components of an idele representing this class.

Local Archimedean

If $F \approx \mathbb{C}$, then $W_F = F^*$ and φ is the trivial map, and r_F is the identity.

If $F \approx \mathbb{R}$, we can take $W_F = \bar{F}^* \cup j\bar{F}^*$ with the rules $j^2 = -1$ and $jcj^{-1} = \bar{c}$, where $c \mapsto \bar{c}$ is the nontrivial element of $\text{Gal}(\bar{F}/F)$. The map φ takes $\bar{F}^*$ to 1 and $j\bar{F}^*$ to that nontrivial

element. The map $r_{\bar{F}}$ is the identity, and r_F is characterized by

$$r_F(-1) = jW_F^c,$$

$$r_F(x) = \sqrt{x}W_F^c, \quad \text{for } x \in F, x > 0.$$

($W_{\bar{F}}^c$ is the “unit circle” of elements $u \in \bar{F}$ with $\|u\| = N_{\bar{F}/F}u = 1$.)

Global Archimedean - Number Field

This is the only case in which there is, at present, no simple description of W_F , but merely the artificial construction by cocycles described in cohomological construction of Weil groups above. This construction is due to Weil in [96], where he emphasizes the importance of the problem of finding a more natural construction, and proves the following facts.

The map $\varphi : W_F \rightarrow G_F$ is surjective. Its kernel is the connected component of identity in W_F , isomorphic to the inverse limit, under the norm maps $N_{E/E'}$ of the connected components D_E of 1 in C_E . These norm maps $D_E \rightarrow D_{E'}$ are surjective, and $r_E(D_E) = (\text{Ker } \varphi)W_E^c/W_E^c$ is the image of $\text{Ker } \varphi$ in $W_{E/F}$.

If E has r_1 real and r_2 complex places then D_E is isomorphic to the product of $\mathbb{R}$ with $r_1 + r_2 - 1$ solenoids and r_2 circles.

Further Comments

(1 .4.5) Notice that in each of the four cases just discussed the subgroups of W_F which are of the form W_E for some finite extension E of F are just the open subgroups of finite index. Their intersection, $\text{Ker } \varphi$, is a divisible connected abelian group, trivial in the first two cases, isomorphic to $\mathbb{C}^*$ in the third, and enormous in the last case. (1 .4.6) In each case there is a homomorphism $w \mapsto \|w\|$ of W_F into the multiplicative group of strictly positive real numbers which reflects the norm or normed absolute value on C_F under the isomorphism $r_F : C_F \rightarrow W_F^{\text{ab}}$. By (1 . 1 .2) and the rule $\|N_{E/F}(a)\|_F = \|a\|_E$, the restriction of this “norm” function $\|w\|$ from W_F to a subgroup W_E is the norm function for W_E , so we can write simply $\|w\|$ instead of $\|w\|_F$ without creating confusion. In each case the kernel W_F^1 of $w \mapsto \|w\|$ is compact. In the first two cases, the image of $w \mapsto \|w\|$ consists of the powers of q_F , and W_F is a semidirect product $Z \ltimes W_F^1$. In the last two cases $w \mapsto \|w\|$ is surjective, and in fact, W_F is a direct product $\mathbb{R} \times W_F^1$. Let us refer to the first two cases as

the “**Z**–cases” and the last two as the “**R**–cases”. In the **Z**–cases, φ is injective, but not surjective ; in the **R**–cases, φ is surjective, but not injective.

7.1.6. Automorphisms of Weil Group

Let W_F be a Weil group for $\bar{F}/F$. Let

$$\text{Aut}(\bar{F}, W_F) = \{(\sigma, \alpha) \in G_F \times \text{Aut}(W_F) \mid \varphi \circ \alpha = \text{Inn}(\alpha) \circ \varphi \text{ and } r_{E^\sigma} \circ \tilde{\sigma} = \tilde{\alpha} \circ r_E\},$$

i.e. the following diagrams are commutative, the second for all E :

$$\begin{array}{ccc} W_F & \xrightarrow{\varphi} & G_F \\ \alpha \downarrow & & \downarrow \text{Inn}(\alpha) \\ W_F & \xrightarrow{\varphi} & G_F \end{array} \quad \text{and} \quad \begin{array}{ccc} C_E & \xrightarrow{r_E} & W_E^{\text{ab}} \\ \tilde{\sigma} \downarrow & & \downarrow \tilde{\alpha} \\ C_{E^\sigma} & \xrightarrow{r_{E^\sigma}} & W_{E^\sigma}^{\text{ab}} \end{array}$$

Here $\text{Inn}(\alpha)$ denotes the inner automorphism defined by α .

We shall call an automorphism of W_F essentially inner if it induces an inner automorphism on $W_{E/F}$ for each finite Galois E/F .

7.1.7. Local-Global Relationship

Suppose F is global. Let ν be a place of F and F_ν be the completion of F at ν . Let $\bar{F}$ (resp. $\bar{F}_\nu$) be a separable algebraic closure of F (resp. F_ν) and let W_F (resp. W_{F_ν}) be a Weil group for $\bar{F}/F$ (resp. $\bar{F}_\nu/F_\nu$).

Proposition 12 *Let $i_\nu : \bar{F} \rightarrow \bar{F}_\nu$ be an F –homomorphism. For each finite extension E of F in $\bar{F}$, let $E_\nu = i_\nu(E)F_\nu$ be the induced completion of E . There exists a continuous homomorphism $\theta_\nu : W_{F_\nu} \rightarrow W_F$ such that the following diagrams are commutative:*

$$\begin{array}{ccc} W_{F_\nu} & \longrightarrow & G_{F_\nu} \\ \theta_\nu \downarrow & & \downarrow i_\nu \\ W_F & \longrightarrow & G_F \end{array} \quad \text{and} \quad \begin{array}{ccc} E_\nu^* & \xrightarrow{\sim} & W_{E_\nu}^{\text{ab}} \\ n_\nu \downarrow & & \downarrow \tilde{i}_\nu \\ C_E & \xrightarrow{\sim} & W_E^{\text{ab}} \end{array}$$

where n_ν maps $a \in E_\nu^*$ to the class of the idele whose ν –component is a and whose other components are 1.

Remark If F is a function field, then θ_ν is unique. In the number field case, θ_ν is unique up

to composition with an inner automorphism of W_F defined by an element of the connected component $W_F^0 = \text{Ker}\varphi$.

Corollary 4 *The diagram*

$$\begin{array}{ccc} W_{F_\nu} & \longrightarrow & G_{F_\nu} \\ \theta_\nu \downarrow & & \downarrow i_\nu \\ W_F & \longrightarrow & G_F \end{array}$$

is unique up to isomorphism, and the automorphisms of it are the inner automorphisms of W defined by elements $w \in W^0$ which induce an automorphism of W_{F_ν} (i.e. for ν nonarchimedean, w fixed by G_{F_ν} and for ν archimedean, w a product of an element of W^0 by an element of $(W^0)^{G_{F_\nu}}$).

7.2. ARTIN RECIPROCITY

This is from [76] p 223-226.

If K/F is a finite extension, we will be concerned with two natural homomorphisms:

$$j_{K/F} : C_F \rightarrow C_K \text{ and } N_{K/F} : C_K \rightarrow C_F.$$

The first map is simply that induced by inclusion. The second is the norm homomorphism, which in the global case is induced by

$$(x_v)_v \mapsto \left(\prod_{v|u} N_v(x_v) \right)_u$$

where $N_v : K_v \rightarrow F_u$ is the ordinary norm. Observe that this idele class version of the norm is well-defined: the ordinary version maps integers to integers (cf. Appendix B, Section 2), and Proposition 4-39 shows that elements of K map to elements of F . Note also that according to Exercise 3 below, the image of $N_{K/F}$ is an open subgroup of C_F . Next fix a separable algebraic closure $\bar{F}$ and put

$$\Gamma_K = \text{Gal}(\bar{F}/K)$$

for any extension K/F with $K \subseteq \bar{F}$. To describe the functoriality of Artin reciprocity, we

shall also need two maps on the Galois side. The first is simply the inclusion

$$i_{K/F} : \Gamma_K \rightarrow \Gamma_F.$$

The second, which goes in the opposite direction, is the more subtle transfer map

$$V : \Gamma_F^{\text{ab}} \rightarrow \Gamma_K^{\text{ab}}$$

defined as above on the abelianizations of the domain and codomain.

THEOREM. (Artin Reciprocity) Let F be a global field or a local field. Then there exists a homomorphism, called the Artin map,

$$\theta_F : C_F \rightarrow \text{Gal}(\bar{F}/F)^{\text{ab}} = \Gamma_F^{\text{ab}}$$

satisfying each of the following two groups of assertions:

PART ONE-The Artin Map for Abelian Extensions

- (i) For every finite abelian extension K/F , let $\theta_{K/F}$ denote the composition of θ_F with the natural projection $\Gamma_F^{\text{ab}} \rightarrow \text{Gal}(K/F)$. Then $\theta_{K/F}$ is surjective with kernel $N_{K/F}(C_K)$.
- (ii) Conversely, given any open subgroup N of C_F of finite index, there exists a finite abelian extension K/F such that $N = \text{Ker}(\theta_{K/F})$. In particular,

$$C_F/N \cong \text{Gal}(K/F).$$

- (iii) Let K/F be a finite abelian and unramified extension of the non-Archimedean local field F with residual extension k'/k . Then we have explicitly

$$\theta_{K/F}(x) = \varphi^{\nu(x)}$$

where φ is the Frobenius element of $\text{Gal}(K/F) \cong \text{Gal}(k'/k) = \langle \varphi \rangle$.

- (iv) Let K/F be a finite abelian extension of global fields, and let P be a finite prime in F that is unramified in K . Denote by x_P the class in C_F defined by the idele

$$\tilde{x}_P = (1, \dots, 1, \pi, 1, \dots, 1)$$

where $(\tilde{x}_P)_P = \pi$, i.e. all of whose components are 1 except at the place defined by

P , where the component is a uniformizing parameter π . Then we have

$$\theta_{K/F}(x_P) = \varphi_P$$

where $\varphi_P = (P, K/F)$. [Note that since K/F is abelian, the Frobenius conjugacy class φ_P is in fact a single element of $\text{Gal}(K/F)$.]

PART TWO-Functoriality

Let K/F be a finite separable extension, not necessarily abelian (with F either global or local). Then we have the following two commutative diagrams:

(i)

$$\begin{array}{ccc} C_K & \xrightarrow{\theta_K} & \Gamma_K^{\text{ab}} \\ N_{K/F} \downarrow & & \downarrow i_{K/F} \\ C_F & \xrightarrow{\theta_F} & \Gamma_F^{\text{ab}} \end{array}$$

(ii)

$$\begin{array}{ccc} C_K & \xrightarrow{\theta_K} & \Gamma_K^{\text{ab}} \\ j_{K/F} \uparrow & & \uparrow V \\ C_F & \xrightarrow{\theta_F} & \Gamma_F^{\text{ab}} \end{array}$$

(iii) Moreover, if K_1/F is an abelian extension with subextension K/F , then we have a further commutative diagram

$$\begin{array}{ccc} F^*/N_{K_1/F}(K_1^*) & \xrightarrow{\theta_{K_1/F}} & \text{Gal}(K_1/F) \\ \downarrow & & \downarrow \\ F^*/N_{K/F}(K^*) & \xrightarrow{\theta_{K/F}} & \text{Gal}(K/F) \end{array}$$

Note well that the inclusion-induced map on the class group side corresponds to the transfer map on the Galois side and that the inclusion map on the Galois side corresponds to the norm map on the class group side. In the abelian case, we may simply identify the projections.

7.2.1. Reciprocity Law isomorphism and Norm-Residue Map

The isomorphism $C_F/N_{K/F}C_K \cong \text{Gal}(K/F)^{\text{ab}}$ is known as the reciprocity law isomorphism. It is the isomorphism between

$$H^0(\text{Gal}(K/F), C_K) \cong H^{-2}(\text{Gal}(K/F), \mathbb{Z})$$

provided by the cup product with the fundamental class of the extension

$$(W6) \quad 1 \longrightarrow C_K \longrightarrow W_{K/F} \longrightarrow \text{Gal}(K/F) \longrightarrow 1$$

The surjective homomorphism $C_F \rightarrow \text{Gal}(K/F)^{\text{ab}}$ with kernel $N_{K/F}C_K$ (induced from the reciprocity law isomorphism above) is called the norm-residue map (symbol), and is denoted by $a \mapsto (a, K/F)$.

Denoting by

$$\mathcal{H} : C_F \rightarrow H^0(\text{Gal}(K/F), C_K)$$

the onto map with kernel $N_{F/K}C_K$, and

$$\zeta : G_{K/F} \rightarrow H^{-2}(G_{K/F}, \mathbb{Z})$$

with kernel $G_{K/F}^c$ and

$$\alpha_{-2}(K/F) : H^{-2}(G_{K/F}, \mathbb{Z}) \rightarrow H^0(\text{Gal}(K/F), C_K)$$

the isomorphism provided by taking cup product with the fundamental class $\alpha_{K/F}$, we have the multi-valued correspondence

$$a \leftrightarrow \sigma \quad a \in C_F \quad \sigma \in G_{K/F}$$

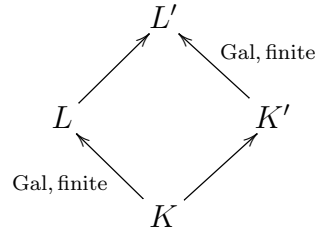
if

$$\mathcal{H}a = \alpha_{-2}(K/F)(\zeta(\sigma)) = \alpha_{K/F} \cdot \zeta(\sigma)$$

The following is from Neukirch class field theory p 29-30.

Proposition 13 *If L/K and L'/K' are finite Galois extensions such that $K \subseteq K'$ and*

$L \subseteq L'$ i.e.



and $\sigma \in G = G_k$, (where $k \leq K, L, K', L' \leq \bar{k}$) we have the commutative diagrams:

$$\begin{array}{ccc}
 C_{K'} \xrightarrow{(\cdot, L'/K')} G(L'/K')^{\text{ab}} & & \\
 \downarrow N_{K'/K} & \text{cores}_L \downarrow & \\
 C_K \xrightarrow{(\cdot, L/K)} G(L/K)^{\text{ab}} & & \\
 \sigma \downarrow & & \tilde{\sigma} \downarrow \\
 C_{K^\sigma} \xrightarrow{(\cdot, L^\sigma/K^\sigma)} G(L^\sigma/K^\sigma)^{\text{ab}} & &
 \end{array}$$

and if $K' \subseteq L$,

$$\begin{array}{ccc}
 C_{K'} \xrightarrow{(\cdot, L/K')} G(L/K')^{\text{ab}} & & \\
 \uparrow & \text{transfer} \uparrow & \\
 C_K \xrightarrow{(\cdot, L/K)} G(L/K)^{\text{ab}} & &
 \end{array}$$

There is a similar statement in Artin-Tate's Class Field Theory [93].

Theorem 16 Using the symbol $\updownarrow (K/F)$ to denote the many valued correspondence inducing the reciprocity law isomorphism in the layer K/F , we assert that the following diagrams are commutative:

(a)

$$\begin{array}{ccc}
 C_F & \xrightarrow{\text{inclusion}} & C_E \quad (F \subset E \subset K) \\
 \updownarrow (K/F) & & \updownarrow (K/E) \\
 G_{K/F}^{\text{ab}} & \xrightarrow{\text{transfer}} & G_{K/E}^{\text{ab}}
 \end{array}$$

(b)

$$\begin{array}{ccc}
C_F & \xleftarrow{N_{E/F}} & C_E \\
(K/F) \downarrow & & \downarrow (K/E) \\
G_{K/F} & \xleftarrow{\text{inclusion}} & G_{K/E}
\end{array} \quad (F \subset E \subset K)$$

(c)

$$\begin{array}{ccc}
C_F & \xrightarrow{\tau} & C_{F^\tau} \\
(K/F) \downarrow & & \downarrow (K^\tau/F^\tau) \\
G_{K/F} & \xrightarrow{\text{Conj}(\tau)} & G_{K^\tau/E^\tau}
\end{array} \quad (F \subset K \ \tau \in G)$$

where $\text{Conj}(\tau)(\sigma) = \tau\sigma\tau^{-1}$ is conjugation by τ .

(d)

$$\begin{array}{ccc}
C_F & \xrightarrow{\text{identity}} & C_F \\
(L/F) \downarrow & & \downarrow (K/F) \\
G_{L/F} & \xrightarrow{\pi} & G_{K/F}
\end{array} \quad (F \subset K \subset L)$$

where $\pi : G_{L/F} \rightarrow G_{L/F}/G_{L/K} = G_{K/F}$ is natural homomorphism onto factor group.

Theorem 17 a) If $F \subset E \subset K$, then for $a \in C_F$ we have

$$(\iota(a), K/E) = V_{G_{K/F}, G_{K/E}}(a, K/F)$$

where $\iota : C_F \rightarrow C_E$ is inclusion.

b) If $F \subset E \subset K$, then for $a \in C_E$ we have

$$(N_{E/F}a, K/F) = (a, K/E) \cdot G_{K/F}^c.$$

c) If $F \subset K$ and $\tau \in G$, then for $a \in C_F$ we have

$$(a^\tau, K^\tau/F^\tau) = (a, K/F)^\tau.$$

d) If $F \subset K \subset L$, and $a \in C_F$, then

$$(a, K/F) = (a, L/F) \cdot G_{L/K}.$$

7.2.2. Abelian Extensions and Norm Groups

Definition 165 An extension M/F is abelian if it is normal and $\text{Gal}(M/F)$ is abelian, i.e. $\text{Gal}(M/k) \supset \text{Gal}(F/k)^c$

Theorem 18 The norm group of an arbitrary extension E/F is the same as that of its maximal abelian subextension M/F , i.e. $N_{E/F}C_E = N_{M/F}C_M$. If $\{M\}$ is the set of all abelian extensions of F then the correspondence $M \leftrightarrow N_{M/F}C_M$ is a one-to-one correspondence between $\{M\}$ and the set of all norm subgroups of C_F , having the following properties:

- (a) $M_1 \subset M_2 \Leftrightarrow N_{M_1/F}C_{M_1} \supset N_{M_2/F}C_{M_2}$
- (b) $N_{M_1M_2/F}C_{M_1M_2} = N_{M_1/F}C_{M_1} \cap N_{M_2/F}C_{M_2}$
- (c) $[M : F] = (C_F : N_{M/F}C_M)$

Every subgroup of C_F which contains a norm subgroup is a norm subgroup.

7.2.3. Weil Group as in Shih

This section treats the exact sequence regarding Weil group in [66].

$L \subset \bar{\mathbb{Q}}$ is a finite Galois extension of $\mathbb{Q}$. We have the following commutative diagrams:

$$\begin{array}{ccccccc} 1 & \longrightarrow & L_v^\times & \longrightarrow & W_{L_v/\mathbb{Q}_v} & \longrightarrow & \text{Gal}(L_v/\mathbb{Q}_v) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & C_L & \longrightarrow & W_{L/\mathbb{Q}} & \longrightarrow & \text{Gal}(L/\mathbb{Q}) \longrightarrow 1 \end{array}$$

This is a combination of the exact sequence in (W6) 7.1.2 and local-global relationship, Proposition 12. The middle map is induced by the map in (proposition 12).

$$\begin{array}{ccccccc} 1 & \longrightarrow & C_L & \longrightarrow & W_{L/\mathbb{Q}} & \longrightarrow & \text{Gal}(L/\mathbb{Q}) \longrightarrow 1 \\ & & \downarrow NR & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \text{Gal}(L^{\text{ab}}/L) & \longrightarrow & \text{Gal}(L^{\text{ab}}/\mathbb{Q}) & \longrightarrow & \text{Gal}(L/\mathbb{Q}) \longrightarrow 1 \end{array}$$

The first line is referred as (W6). The first vertical map is the Norm-Residue map. Note

that norm-residue map arises from the reciprocity law isomorphism $C_L/N_{L^{\text{ab}}/L}C_{L^{\text{ab}}} \cong \text{Gal}(L^{\text{ab}}/L)^{\text{ab}} = \text{Gal}(L^{\text{ab}}/L)$.

By reciprocity, $\text{Gal}(L^{\text{ab}}/\mathbb{Q})^{\text{ab}} \cong C_{\mathbb{Q}}/N_{L^{\text{ab}}/\mathbb{Q}}C_{L^{\text{ab}}}$ Therefore the norm residue map

$$NR_{L^{\text{ab}}/\mathbb{Q}} : C_{\mathbb{Q}} \rightarrow \text{Gal}(L^{\text{ab}}/\mathbb{Q})^{\text{ab}}$$

But $C_{\mathbb{Q}}$ is isomorphic to $W_{\mathbb{Q}}^{\text{ab}}$, via $r_{\mathbb{Q}}$. Furthermore, $W_{\mathbb{Q}}^{\text{ab}} = W_{\mathbb{Q}}/W_{\mathbb{Q}}^c$ and $W_{L/\mathbb{Q}} = W_{\mathbb{Q}}/W_L^c$. Therefore we can project from $W_{L/\mathbb{Q}}$ onto $W_{\mathbb{Q}}^{\text{ab}}$.

Therefore we have the following diagram:

$$\begin{array}{ccccc}
 & & & W_L^{\text{ab}} & \\
 & & r_L \nearrow & \downarrow \iota & \\
 C_L & \xrightarrow{\iota \circ r_L} & W_{L/\mathbb{Q}} & \downarrow \pi & \\
 & & & W_{\mathbb{Q}}^{\text{ab}} & \\
 & & N_{L/\mathbb{Q}} \searrow & \downarrow r_{\mathbb{Q}}^{-1} & \\
 & & & C_{\mathbb{Q}} & \\
 & & & \downarrow NR_{L^{\text{ab}}/\mathbb{Q}} & \\
 & & & \text{Gal}(L^{\text{ab}}/\mathbb{Q})^{\text{ab}} & \\
 NR_{L^{\text{ab}}/L} \downarrow & & & & \\
 \text{Gal}(L^{\text{ab}}/L) & \longrightarrow & & &
 \end{array}$$

The commutativity of the lower part, follows from a property satisfied by the norm-residue symbol.

Since by (W5) we have the commutative diagram:

$$\begin{array}{ccc}
 C_L & \xrightarrow{r_L} & W_L^{\text{ab}} \\
 N_{L/\mathbb{Q}} \downarrow & & \downarrow \tilde{\iota} \\
 C_{\mathbb{Q}} & \xrightarrow{r_{\mathbb{Q}}} & W_{\mathbb{Q}}^{\text{ab}}
 \end{array}$$

Note that $\tilde{\iota} : W_L^{\text{ab}} \rightarrow W_{\mathbb{Q}}^{\text{ab}}$ is induced from the inclusion $\mathbb{Q} \hookrightarrow L$. and we have the

commutative diagram:

$$\begin{array}{ccccc}
 W_L^{\text{ab}} & \xleftarrow{\pi^{\text{ab}}} & W_L & \xrightarrow{\varphi} & G_L \\
 \downarrow \tilde{\iota} & & \downarrow \iota & & \downarrow \iota \\
 W_{\mathbb{Q}}^{\text{ab}} & \xleftarrow{\pi^{\text{ab}}} & W_{\mathbb{Q}} & \xrightarrow{\varphi} & G_{\mathbb{Q}}
 \end{array}$$

evidently

$$\begin{array}{ccc}
 & W_L^{\text{ab}} & \\
 \swarrow \iota & & \downarrow \tilde{\iota} \\
 W_{L/\mathbb{Q}} & & W_{\mathbb{Q}}^{\text{ab}} \\
 \searrow \pi & & \\
 & &
 \end{array}$$

is commutative, as

$$\begin{array}{ccccc}
 & W_L^{\text{ab}} & \xleftarrow{\pi^{\text{ab}}} & W_L & \\
 \swarrow \iota & \downarrow \tilde{\iota} & & \downarrow \iota & \\
 W_{L/\mathbb{Q}} & & & & \\
 \searrow \pi & & W_{\mathbb{Q}}^{\text{ab}} & \xleftarrow{\pi^{\text{ab}}} & W_{\mathbb{Q}}
 \end{array}$$

As $(W_{\mathbb{Q}}/W_{\mathbb{Q}}^c) = (W_{\mathbb{Q}}/W_L^c)/(W_{\mathbb{Q}}^c/W_L^c)$ and we have the commutative diagram:

$$\begin{array}{ccccc}
 W_L^{\text{ab}} & \xleftarrow{\pi^{\text{ab}}} & W_L & & \\
 \downarrow \iota & & \downarrow \iota & & \\
 W_{L/\mathbb{Q}} & \xleftarrow{\pi} & W_{\mathbb{Q}} & & \\
 \downarrow \pi & \nearrow \pi^{\text{ab}} & & & \\
 W_{\mathbb{Q}}^{\text{ab}} & & & &
 \end{array}$$

Therefore we have that the composition

$$W_L^{\text{ab}} \xrightarrow{\iota} W_{L/\mathbb{Q}} \xrightarrow{\pi} W_{\mathbb{Q}}^{\text{ab}}$$

is same as inclusion of $W_L^{\text{ab}} \rightarrow W_{\mathbb{Q}}^{\text{ab}}$

On the other hand, the map

$$W_{L/\mathbb{Q}} \rightarrow \text{Gal}(L/\mathbb{Q})$$

is the composition

$$W_{L/\mathbb{Q}} = W_{\mathbb{Q}}/W_L^c \xrightarrow{\pi} W_{\mathbb{Q}}/W_L \xrightarrow{\tilde{\varphi}} \text{Gal}(L/\mathbb{Q})$$

Now putting things together, we have:

$$\begin{array}{ccccc}
 & & W_{L/\mathbb{Q}} & \xrightarrow{\quad} & W_{\mathbb{Q}}/W_L \xrightarrow{\tilde{\varphi}} \text{Gal}(L/\mathbb{Q}) \\
 & \nearrow \iota & \searrow \pi & & \\
 W_L^{\text{ab}} & \xrightarrow{\quad \iota \quad} & W_{\mathbb{Q}}^{\text{ab}} & & \\
 \uparrow r_L & & \uparrow r_{\mathbb{Q}} & & \\
 C_L & \xrightarrow{N_{L/\mathbb{Q}}} & C_{\mathbb{Q}} & \xrightarrow{\text{id}} & C_{\mathbb{Q}} \\
 \downarrow NR_{L^{\text{ab}}/L} & & \downarrow NR_{L^{\text{ab}}/\mathbb{Q}} & & \downarrow NR_{L/\mathbb{Q}} \\
 \text{Gal}(L^{\text{ab}}/L) & \xrightarrow{\quad \iota \quad} & \text{Gal}(L^{\text{ab}}/\mathbb{Q})^{\text{ab}} & \xrightarrow{\pi} & \text{Gal}(L/\mathbb{Q})^{\text{ab}}
 \end{array}$$

But now we also have the commutative diagram:

$$\begin{array}{ccccc}
 C_L & \xrightarrow{r_L} & W_L^{\text{ab}} & \xrightarrow{\varphi^{\text{ab}}} & \text{Gal}(\bar{\mathbb{Q}}/L)^{\text{ab}} \\
 \downarrow N_{L/\mathbb{Q}} & & \downarrow \iota & & \downarrow \iota \\
 C_{\mathbb{Q}} & \xrightarrow{r_{\mathbb{Q}}} & W_{\mathbb{Q}}^{\text{ab}} & \xrightarrow{\varphi^{\text{ab}}} & \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})^{\text{ab}} \\
 \downarrow & & & & \downarrow \\
 C_{\mathbb{Q}} & \xrightarrow{NR_{L/\mathbb{Q}}} & & & \text{Gal}(L/\mathbb{Q})^{\text{ab}}
 \end{array}$$

By (W1) the middle and top lines are the Artin reciprocity map.

In fact we can (probably) form the commutative diagram:

$$C_{\mathbb{Q}}/N_{L/\mathbb{Q}}C_L \xrightarrow{\tilde{r}} W_{\mathbb{Q}}^{\text{ab}}/W_L^{\text{ab}} \xrightarrow{\tilde{\varphi}} \text{Gal}(L/\mathbb{Q})^{\text{ab}}$$

On the other hand, the right hand side of the previous commutative diagram can be completed as follows (though maybe this is not that obvious):

$$\begin{array}{ccccccc}
C_L & \xrightarrow{r_L} & W_L^{\text{ab}} & \xrightarrow{\pi} & W_{L/\mathbb{Q}} & \xrightarrow{\pi} & W_{\mathbb{Q}}/W_L \xrightarrow{\tilde{\varphi}} \text{Gal}(L/\mathbb{Q}) \\
\downarrow NR_{L^{\text{ab}}/L} & & \downarrow \iota^{\text{ab}} & & \downarrow \pi & & \downarrow \pi^{\text{ab}} \\
& & W_{\mathbb{Q}}^{\text{ab}} & \xrightarrow{\pi} & W_{\mathbb{Q}}^{\text{ab}}/W_L^{\text{ab}} & & \\
& & \downarrow r_{\mathbb{Q}}^{-1} & & \uparrow \tilde{r} & & \\
& & C_{\mathbb{Q}} & & & & \\
& & \downarrow NR_{L^{\text{ab}}/\mathbb{Q}} & & \searrow NR_{L/\mathbb{Q}} & & \\
\text{Gal}(L^{\text{ab}}/L) & \longrightarrow & \text{Gal}(L^{\text{ab}}/\mathbb{Q})^{\text{ab}} & \xrightarrow{\pi} & \text{Gal}(L/\mathbb{Q})^{\text{ab}} & &
\end{array}$$

$$\begin{array}{ccccccc}
& & W_L^{\text{ab}} & & W_{\mathbb{Q}}/W_L & & \\
& \nearrow r_L & \searrow \iota & \nearrow \pi & \searrow \tilde{\varphi} & & \\
1 \longrightarrow & C_L & \longrightarrow & W_{L/\mathbb{Q}} & \longrightarrow & \text{Gal}(L/\mathbb{Q}) & \longrightarrow 1 \\
& \downarrow & & \downarrow & & \downarrow & \\
& \text{Gal}(L^{\text{ab}}/L) & \xrightarrow{\iota} & \text{Gal}(L^{\text{ab}}/\mathbb{Q})^{\text{ab}} & \xrightarrow{\pi} & \text{Gal}(L/\mathbb{Q})^{\text{ab}} &
\end{array}$$

Remark The argument given here does not yield the commutative diagram of exact sequences stated in Shih [66]. The argument is concluded in Section 7.6, where the diagram of exact sequences that appears in Shih is derived.

7.3. NOTATION

F a field (local or global). $\bar{F}$: separable algebraic closure.

$$G_X = \text{Gal}(\bar{F}/X)$$

$W_X = \varphi^{-1}(G_X)$ where $\varphi : W_F \rightarrow G_F$ is continuous and $F \leq X \leq \bar{F}$.

$\varphi_X : W_X \rightarrow G_X$ so that $\iota \circ \varphi_X = \varphi \circ \iota$, where ι being inclusion.

$$W_{X/Y} = W_Y/W_X^c \text{ for } F \leq X \leq Y \leq \bar{F}.$$

$r_X : C_X \rightarrow W_X^{\text{ab}}$ for $F \leq X \leq \bar{F}$, isomorphisms, such that

(W1) $\varphi_X^{\text{ab}} \circ r_X : C_X \rightarrow G_X^{\text{ab}}$ is Artin-reciprocity map.

7.4. RELATIVE WEIL GROUP AND WEIL GROUP QUOTIENTS

$$F \subseteq E_1 \subseteq E_2 \subseteq E_3 \subseteq \bar{F}$$

Then we have $W_F \supseteq W_{E_1} \supseteq W_{E_2} \supseteq W_{E_3} \supseteq W_{\bar{F}}$ and

$$G_F \supseteq G_{E_1} \supseteq G_{E_2} \supseteq G_{E_3} \supseteq G_{\bar{F}} = \{e\}$$

Then we have

$$\begin{array}{ccc} 1 & & 1 \\ \downarrow & & \downarrow \\ W_{E_2}/W_{E_3} & \longrightarrow & G_{E_2}/G_{E_3} \\ \downarrow & & \downarrow \\ W_{E_1}/W_{E_3} & \longrightarrow & G_{E_1}/G_{E_3} \\ \downarrow & & \downarrow \\ W_{E_1}/W_{E_2} & \longrightarrow & G_{E_1}/G_{E_2} \\ \downarrow & & \downarrow \\ 1 & & 1 \end{array}$$

Also we have the inclusion:

$$\iota_{2,1}^3 : W_{E_3/E_2} \rightarrow W_{E_3/E_1}$$

induced from the inclusion $\iota : W_{E_2} \rightarrow W_{E_1}$, with quotient by $W_{E_3}^c$. and the projection:

$$\pi_1^{3,2} : W_{E_3/E_1} \rightarrow W_{E_2/E_1}$$

induced from the inclusion $\iota : W_{E_3} \rightarrow W_{E_2}$ which induces the inclusion $\iota : W_{E_3}^c \rightarrow W_{E_2}^c$.

The cokernel of the inclusion is W_{E_1}/W_{E_2}

The kernel of the projection is $W_{E_2}^c/W_{E_3}^c$. which may be identified with W_{E_3/E_2}^c .

This means that we have the exact sequences:

$$1 \longrightarrow W_{E_3/E_2} \xrightarrow{\iota} W_{E_3/E_1} \xrightarrow{\pi} W_{E_1}/W_{E_2} \longrightarrow 1$$

and

$$1 \longrightarrow W_{E_2}^c/W_{E_3}^c = W_{E_3/E_2}^c \xrightarrow{\iota} W_{E_3/E_1} \xrightarrow{\pi} W_{E_2/E_1} \longrightarrow 1$$

Furthermore, since $W_{E_2}^c \subseteq W_{E_2}$, we have the projection

$$W_{E_2/E_1} \rightarrow W_{E_1}/W_{E_2}.$$

which has kernel, $W_{E_2}^{\text{ab}} = W_{E_2}/W_{E_2}^c$.

This gives the commutative diagram below:

$$\begin{array}{ccccccc}
 & & 1 & & & & \\
 & & \uparrow & & & & \\
 & & W_{E_2}^{\text{ab}} & & & & \\
 & & \uparrow \pi & & & & \\
 1 & \longrightarrow & W_{E_3/E_2} & \xrightarrow{\iota} & W_{E_3/E_1} & \xrightarrow{\pi} & W_{E_1}/W_{E_2} \longrightarrow 1 \\
 & & \uparrow \iota & & \uparrow \text{id} & & \uparrow \pi \\
 1 & \longrightarrow & W_{E_2}^c/W_{E_3}^c & \xrightarrow{\iota} & W_{E_3/E_1} & \xrightarrow{\pi} & W_{E_2/E_1} \longrightarrow 1 \\
 & & \uparrow & & \uparrow & & \uparrow \iota \\
 & & 1 & & 1 & & W_{E_2}^{\text{ab}} \\
 & & & & & & \uparrow \\
 & & & & & & 1
 \end{array}$$

Note that from the above diagram that there is a group homomorphism

$$W_{E_3/E_2} \rightarrow W_{E_2/E_1}$$

given by the composition

$$W_{E_3/E_2} \xrightarrow{\pi} W_{E_2}^{\text{ab}} \xrightarrow{\iota} W_{E_2/E_1}$$

and also from the composition

$$W_{E_3/E_2} \xrightarrow{\iota} W_{E_3/E_1} \xrightarrow{\pi} W_{E_2/E_1}$$

Since these simply change the order of inclusion and taking quotient, they are identical, which gives the commutative square:

$$\begin{array}{ccc}
W_{E_3/E_2} & \xrightarrow{\pi} & W_{E_2}^{\text{ab}} \\
\downarrow \iota & & \downarrow \iota \\
W_{E_3/E_1} & \xrightarrow{\pi} & W_{E_2/E_1}
\end{array}$$

combining with the above:

$$\begin{array}{ccccc}
W_{E_2}^c/W_{E_3}^c & \longrightarrow & W_{E_3/E_2} & \xrightarrow{\pi} & W_{E_2}^{\text{ab}} \\
\downarrow \text{id} & & \downarrow \iota & & \downarrow \iota \\
W_{E_2}^c/W_{E_3}^c & \longrightarrow & W_{E_3/E_1} & \xrightarrow{\pi} & W_{E_2/E_1} \\
& & \downarrow \pi & & \downarrow \pi \\
& & W_{E_1}/W_{E_2} & \xrightarrow{\text{id}} & W_{E_1}/W_{E_2}
\end{array}$$

Now starting with the exact sequence

$$1 \longrightarrow W_{E_2}/W_{E_3} \longrightarrow W_{E_1}/W_{E_3} \longrightarrow W_{E_1}/W_{E_2} \longrightarrow 1$$

and adding one possible tail (and the other tail is already included):

$$\begin{array}{ccccccc}
W_{E_3}^{\text{ab}} & \xrightarrow{\text{id}} & W_{E_3}^{\text{ab}} & \xrightarrow{\iota^{\text{ab}}} & W_{E_2}^{\text{ab}} & & \\
\downarrow \iota & & \downarrow \iota & & \downarrow \iota & & \\
W_{E_3/E_2} & \xrightarrow{\iota} & W_{E_3/E_1} & \xrightarrow{\pi} & W_{E_2/E_1} & & \\
\downarrow \pi & & \downarrow \pi & & \downarrow \pi & & \\
1 \longrightarrow & W_{E_2}/W_{E_3} & \xrightarrow{\iota} & W_{E_1}/W_{E_3} & \xrightarrow{\pi} & W_{E_1}/W_{E_2} & \longrightarrow 1
\end{array}$$

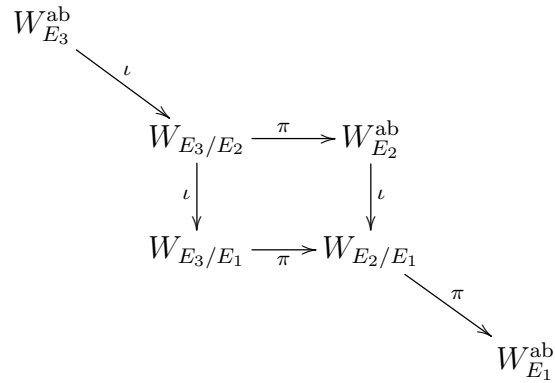
Commutativity of the diagram $W_{E_3}^c \longrightarrow W_{E_2}^c$ gives the commutativity of the right-bottom

$$\begin{array}{ccc}
W_{E_3}^c & \longrightarrow & W_{E_2}^c \\
\downarrow & & \downarrow \\
W_{E_3} & \longrightarrow & W_{E_2}
\end{array}$$

square in the previous diagram, with projection maps.

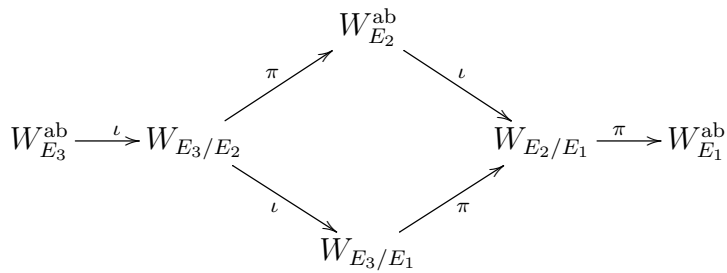
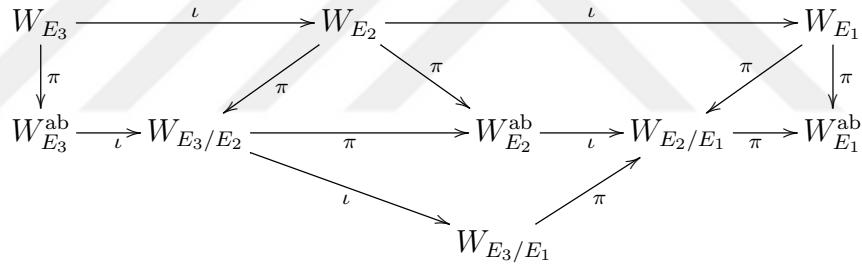
On the other hand, $\iota^{\text{ab}} : W_{E_3}^{\text{ab}} \rightarrow W_{E_2}^{\text{ab}}$ factorizes as $W_{E_3}^{\text{ab}} \xrightarrow{\iota} W_{E_3/E_2} \xrightarrow{\pi} W_{E_2}^{\text{ab}}$ and the

diagram



commutes, since the inclusions are induced from inclusion $W_{E_2} \xrightarrow{\iota} W_{E_3}$ and the projections are induced from the inclusion $W_{E_2}^c \xrightarrow{\iota} W_{E_3}^c$

To be fully convinced also note:



In order to complete the drift of the argument, one can form the more cluttered diagrams below:

$$\begin{array}{ccccccc}
& 1 & & 1 & & 1 & \\
& \downarrow & & \downarrow & & \downarrow & \\
& W_{E_3}^{\text{ab}} & \xrightarrow{\text{id}} & W_{E_3}^{\text{ab}} & \xrightarrow{\iota^{\text{ab}}} & W_{E_2}^{\text{ab}} & \xrightarrow{\iota^{\text{ab}}} & W_{E_1}^{\text{ab}} \\
& \downarrow \iota & & \downarrow \iota & & \downarrow \iota & & \downarrow \iota \\
& W_{E_3/E_2} & \xrightarrow{\iota} & W_{E_3/E_1} & \xrightarrow{\pi} & W_{E_2/E_1} & & \\
& \downarrow \pi & & \downarrow \pi & & \downarrow \pi & & \\
1 \longrightarrow & W_{E_2}/W_{E_3} & \xrightarrow{\iota} & W_{E_1}/W_{E_3} & \xrightarrow{\pi} & W_{E_1}/W_{E_2} & \longrightarrow & 1 \\
& \downarrow & & \downarrow & & \downarrow & & \\
& 1 & & 1 & & 1 & &
\end{array}$$

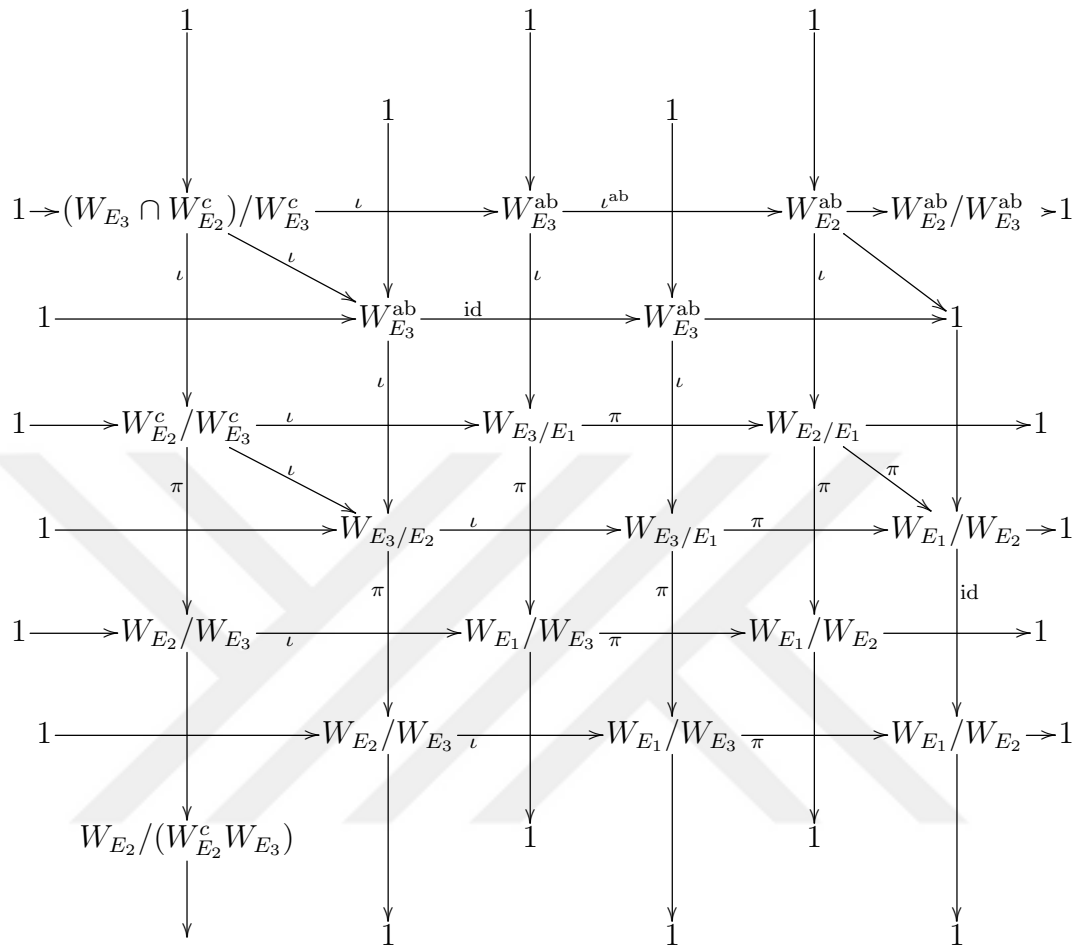
And we have the following exact sequences:

$$\begin{array}{ccccccc}
& 1 & & 1 & & & \\
& \downarrow & & \downarrow & & & \\
1 \longrightarrow & W_{E_3}^{\text{ab}} & \xrightarrow{\text{id}} & W_{E_3}^{\text{ab}} & \longrightarrow & 1 & \\
& \downarrow \iota & & \downarrow \iota & & \downarrow & \\
1 \longrightarrow & W_{E_3/E_2} & \xrightarrow{\iota} & W_{E_3/E_1} & \xrightarrow{\pi} & W_{E_1}/W_{E_2} & \longrightarrow & 1 \\
& \downarrow \pi & & \downarrow \pi & & \downarrow \text{id} & \\
1 \longrightarrow & W_{E_2}/W_{E_3} & \xrightarrow{\iota} & W_{E_1}/W_{E_3} & \xrightarrow{\pi} & W_{E_1}/W_{E_2} & \longrightarrow & 1 \\
& \downarrow & & \downarrow & & \downarrow & \\
& 1 & & 1 & & 1 &
\end{array}$$

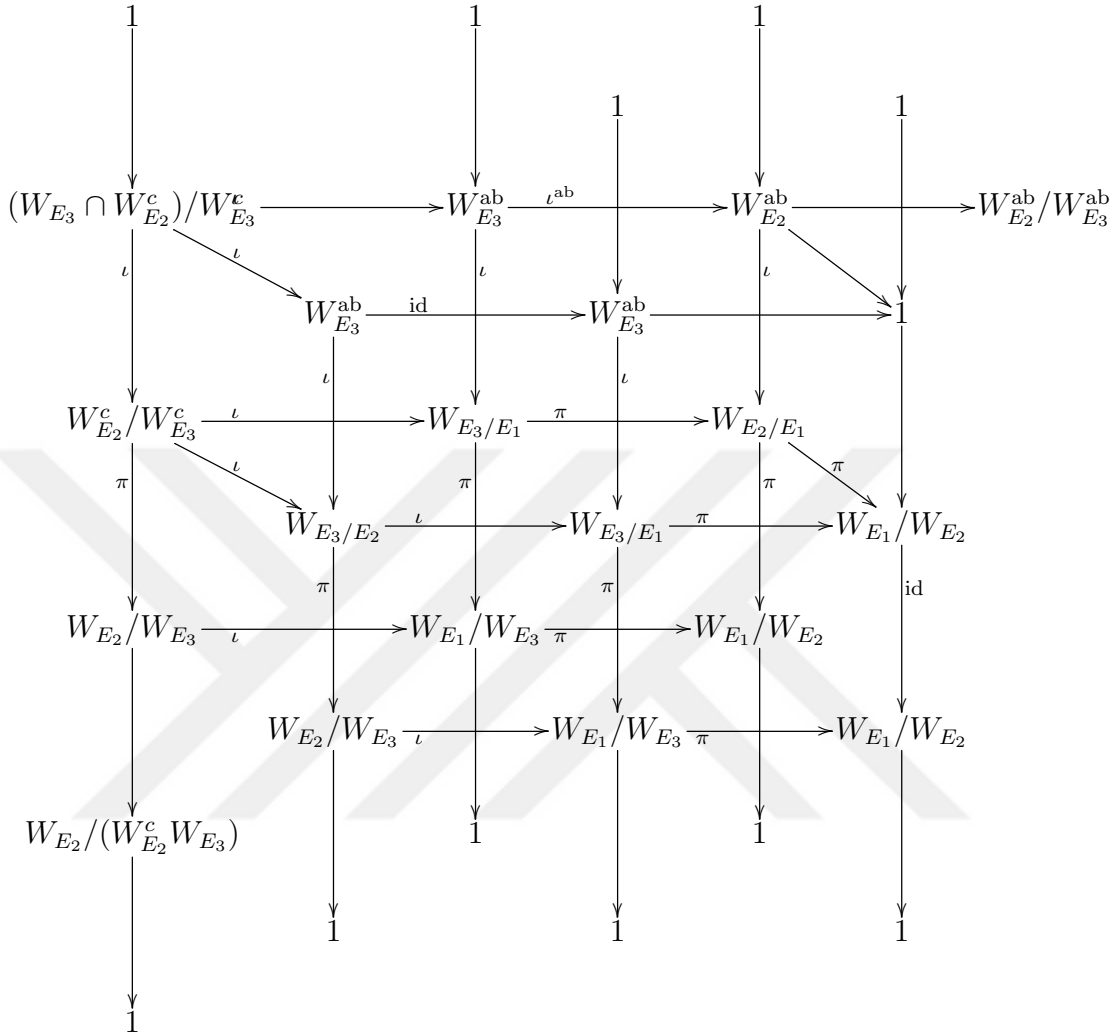
and the following commutative diagram of exact sequences:

$$\begin{array}{ccccccc}
& & 1 & & 1 & & 1 \\
& & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & (W_{E_3} \cap W_{E_2}^c)/W_{E_3}^c & \xrightarrow{\iota} & W_{E_3}^{\text{ab}} & \xrightarrow{\iota^{\text{ab}}} & W_{E_2}^{\text{ab}} \longrightarrow W_{E_2}^{\text{ab}}/W_{E_3}^{\text{ab}} \longrightarrow 1 \\
& & \downarrow \iota & & \downarrow \iota & & \downarrow \iota \\
1 & \longrightarrow & W_{E_2}^c/W_{E_3}^c & \xrightarrow{\iota} & W_{E_3/E_1} & \xrightarrow{\pi} & W_{E_2/E_1} \longrightarrow 1 \\
& & \downarrow \pi & & \downarrow \pi & & \downarrow \pi \\
1 & \longrightarrow & W_{E_2}/W_{E_3} & \xrightarrow{\iota} & W_{E_1}/W_{E_3} & \xrightarrow{\pi} & W_{E_1}/W_{E_2} \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & W_{E_2}/(W_{E_2}^c W_{E_3}) & & 1 & & 1 \\
& & \downarrow & & & & \\
& & 1 & & & &
\end{array}$$

In fact the two diagrams can be put into a single diagram where the first lies above the second.



Redrawing the diagram for visibility:



Focusing on the left side we get:

$$\begin{array}{ccccc}
 W_{E_3} \cap W_{E_2}^c/W_{E_3}^c & \xrightarrow{\iota} & W_{E_3}^{ab} & \xrightarrow{\pi} & W_{E_3}/(W_{E_3} \cap W_{E_2}^c) = W_{E_3}W_{E_2}^c/W_{E_2}^c \\
 \downarrow \iota & & \downarrow \iota & & \downarrow \iota \\
 W_{E_2}^c/W_{E_3}^c & \xrightarrow{\iota} & W_{E_3}/E_2 & \xrightarrow{\pi} & W_{E_2}^{ab}
 \end{array}$$

Note

$$W_{E_2}^c/W_{E_3}^c \longrightarrow W_{E_2}/W_{E_3}$$

decomposes as

$$W_{E_2}^c/W_{E_3}^c \xrightarrow{\iota} W_{E_2}/W_{E_3}^c \xrightarrow{\pi} W_{E_2}/W_{E_3}$$

so we have the commutative diagram

$$\begin{array}{ccccc}
 W_{E_2}^c \cap W_{E_3} / W_{E_3}^c & & & & \\
 \downarrow \iota & \searrow \iota & & & \\
 & W_{E_2}^c / W_{E_3}^c & & & \\
 & \downarrow \iota & \searrow & & \\
 W_{E_3}^{\text{ab}} & \xrightarrow{\iota} & W_{E_2} / W_{E_3}^c & \xrightarrow{\pi} & W_{E_2} / W_{E_3}
 \end{array}$$

Note $\ker \pi \cong W_{E_3}^{\text{ab}}$, and $\iota^{-1}(W_{E_3}^{\text{ab}}) = (W_{E_2}^c \cap W_{E_3}) / W_{E_3}^c$ where $\iota : W_{E_2}^c / W_{E_3}^c \rightarrow W_{E_2} / W_{E_3}^c$

So it seems fair to expect that kernel of $\pi \circ \iota : W_{E_2}^c / W_{E_3}^c \rightarrow W_{E_2} / W_{E_3}$ should be this set. However note that ι is not surjective, hence $\pi \circ \iota$ is not surjective, though π is.

On the other hand

$$\frac{W_{E_2}^c / W_{E_3}^c}{(W_{E_2}^c \cap W_{E_3}) / W_{E_3}^c} \cong W_{E_2}^c / (W_{E_2}^c \cap W_{E_3}) \cong (W_{E_2}^c W_{E_3}) / W_{E_3}$$

Keep in mind that

$$\begin{array}{ccc}
 & W_{E_2} & \\
 & | & \\
 & W_{E_2}^c W_{E_3} & \\
 & / \quad \backslash & \\
 W_{E_2}^c & & W_{E_3} \\
 & \backslash \quad / & \\
 & W_{E_2}^c \cap W_{E_3} & \\
 & | & \\
 & W_{E_3}^c &
 \end{array}$$

Remark: So maybe there is something that does not entirely fit together.

7.5. ATTEMPTS TO COMBINE THE DIAGRAMS OF PREVIOUS SECTION WITH WEIL GROUP DIAGRAMS

Starting with the commutative diagram,

$$\begin{array}{ccccccc}
 & 1 & & 1 & & 1 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & W_{E_3}^{\text{ab}} & \xrightarrow{\text{id}} & W_{E_3}^{\text{ab}} & \xrightarrow{\iota^{\text{ab}}} & W_{E_2}^{\text{ab}} & \xrightarrow{\iota^{\text{ab}}} & W_{E_1}^{\text{ab}} \\
 & \downarrow \iota & & \downarrow \iota & & \downarrow \iota & & \downarrow \iota \\
 & W_{E_3/E_2} & \xrightarrow{\iota} & W_{E_3/E_1} & \xrightarrow{\pi} & W_{E_2/E_1} & & \\
 & \downarrow \pi & & \downarrow \pi & & \downarrow \pi & & \\
 1 & \longrightarrow & W_{E_2}/W_{E_3} & \xrightarrow{\iota} & W_{E_1}/W_{E_3} & \xrightarrow{\pi} & W_{E_1}/W_{E_2} & \longrightarrow 1 \\
 & \downarrow & & \downarrow & & \downarrow & & \\
 & 1 & & 1 & & 1 & &
 \end{array}$$

and utilizing isomorphisms $r_E : C_E \rightarrow W_E^{\text{ab}}$ and $\tilde{\varphi} : W_X/W_Y \rightarrow \text{Gal}(Y/X) \cong G_X/G_Y = \text{Gal}(\bar{F}/X)/\text{Gal}(\bar{F}/Y)$ whenever $F \subseteq X \subseteq Y \subseteq \bar{F}$ and Y a Galois extension over X , and property referred as (W5) we get the following diagram:

$$\begin{array}{ccccccccccc}
 & 1 & & 1 & & 1 & & 1 & & 1 & \\
 & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\
 & W_{E_3}^{\text{ab}} & \xrightarrow{\text{id}} & W_{E_3}^{\text{ab}} & \xrightarrow{\iota^{\text{ab}}} & W_{E_2}^{\text{ab}} & \xrightarrow{\iota^{\text{ab}}} & W_{E_1}^{\text{ab}} & & & \\
 & \downarrow \iota & & \downarrow \iota & & \downarrow \iota & & \downarrow \iota & & \downarrow \iota & \\
 & W_{E_3/E_2} & \xrightarrow{\iota} & W_{E_3/E_1} & \xrightarrow{\pi} & W_{E_2/E_1} & & & & & \\
 & \downarrow \pi & & \downarrow \pi & & \downarrow \pi & & \downarrow \pi & & \downarrow \pi & \\
 1 & \longrightarrow & W_{E_2}/W_{E_3} & \xrightarrow{\iota} & W_{E_1}/W_{E_3} & \xrightarrow{\pi} & W_{E_1}/W_{E_2} & \longrightarrow & 1 & & \\
 & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\
 & 1 & & 1 & & 1 & & 1 & & 1 &
 \end{array}$$

$\xrightarrow{r_{E_3}^{-1}} C_{E_3} \xrightarrow{\pi} W_{E_3/E_2} \xrightarrow{\iota} W_{E_3/E_1} \xrightarrow{\pi} W_{E_2/E_1} \xrightarrow{\pi} 1$
 $\xrightarrow{r_{E_2}^{-1}} C_{E_2} \xrightarrow{\pi} W_{E_2/E_1} \xrightarrow{\pi} 1$
 $\xrightarrow{N_{E_3, E_2}} C_{E_3} \xrightarrow{\pi} W_{E_3/E_1} \xrightarrow{\pi} W_{E_2/E_1} \xrightarrow{\pi} 1$
 $\xrightarrow{\tilde{\varphi}_{2,3}} \text{Gal}(E_3/E_2) \xrightarrow{\tilde{\varphi}_{1,3}} \text{Gal}(E_3/E_1) \xrightarrow{\tilde{\varphi}_{1,2}} \text{Gal}(E_2/E_1) \longrightarrow 1$

In order to see it more clearly the front commutative diagram is reproduced below:

$$\begin{array}{ccccc}
 & 1 & & 1 & & 1 \\
 & \downarrow & & \downarrow & & \downarrow \\
 & C_{E_3} & \xrightarrow{\text{id}} & C_{E_3} & \xrightarrow{N_{E_3/E_2}} & C_{E_2} \\
 \iota_{3,2} \circ r_{E_3} \downarrow & & & \downarrow \iota_{3,1} \circ r_{E_3} & & \downarrow \iota_{2,1} \circ r_{E_2} \\
 W_{E_3/E_2} & \xrightarrow{\iota} & W_{E_3/E_1} & \xrightarrow{\pi} & W_{E_2/E_1} \\
 \downarrow \tilde{\varphi}_{2,3} \circ \pi & & \downarrow \tilde{\varphi}_{1,3} \circ \pi & & \downarrow \tilde{\varphi}_{1,2} \circ \pi \\
 1 \longrightarrow & \text{Gal}(E_3/E_2) & \xrightarrow{\iota} & \text{Gal}(E_3/E_1) & \xrightarrow{\pi} & \text{Gal}(E_2/E_1) \longrightarrow 1 \\
 & \downarrow & & \downarrow & & \downarrow \\
 & 1 & & 1 & & 1
 \end{array}$$

7.6. SOME EXACT SEQUENCES

From the exact sequence: $1 \longrightarrow W_E^{\text{ab}} \longrightarrow W_{E/F} \longrightarrow W_F/W_E \longrightarrow 1$

$$\begin{array}{ccccccc}
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & C_E & \longrightarrow & W_{E/F} & \longrightarrow & \text{Gal}(E/F) \longrightarrow 1
 \end{array}$$

and assuming $K \supset E \supset F$ we get:

$$\begin{array}{ccccccc}
 1 & \longrightarrow & W_K^{\text{ab}} & \longrightarrow & W_{K/F} & \longrightarrow & W_F/W_K \longrightarrow 1 \\
 & & \downarrow & \searrow & \downarrow & \searrow & \downarrow \\
 & 1 & \longrightarrow & W_E^{\text{ab}} & \longrightarrow & W_{E/F} & \longrightarrow W_F/W_E \longrightarrow 1 \\
 & & \downarrow & \searrow & \downarrow & \searrow & \downarrow \\
 1 & \longrightarrow & C_K & \longrightarrow & W_{K/F} & \longrightarrow & \text{Gal}(K/F) \longrightarrow 1 \\
 & & \downarrow N_{K/E} & \searrow & \downarrow & \searrow & \downarrow \\
 & 1 & \longrightarrow & C_E & \longrightarrow & W_{E/F} & \longrightarrow \text{Gal}(E/F) \longrightarrow 1
 \end{array}$$

and

$$\begin{array}{ccccccc}
 1 & \longrightarrow & W_K^{\text{ab}} & \longrightarrow & W_{K/E} & \longrightarrow & W_E/W_K \longrightarrow 1 \\
 & & \downarrow & \searrow & \downarrow & \searrow & \downarrow \\
 & 1 & \longrightarrow & W_K^{\text{ab}} & \longrightarrow & W_{K/F} & \longrightarrow W_F/W_K \longrightarrow 1 \\
 & & \downarrow & \searrow & \downarrow & \searrow & \downarrow \\
 1 & \longrightarrow & C_K & \longrightarrow & W_{K/E} & \longrightarrow & \text{Gal}(K/E) \longrightarrow 1 \\
 & & \downarrow & \searrow & \downarrow & \searrow & \downarrow \\
 & 1 & \longrightarrow & C_K & \longrightarrow & W_{K/F} & \longrightarrow \text{Gal}(K/F) \longrightarrow 1
 \end{array}$$

Setting $K = L^{\text{ab}}$ and $E = L$ and $F = \mathbb{Q}$, and focusing on the lower parts of the two

commutative diagrams above, we obtain the following commutative diagram:

$$\begin{array}{ccccccc}
 1 & \longrightarrow & C_{L^{\text{ab}}} & \longrightarrow & W_{L^{\text{ab}}/L} & \longrightarrow & \text{Gal}(L^{\text{ab}}/L) \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & C_{L^{\text{ab}}} & \longrightarrow & W_{L^{\text{ab}}/\mathbb{Q}} & \longrightarrow & \text{Gal}(L^{\text{ab}}/\mathbb{Q}) \longrightarrow 1 \\
 & & \downarrow N_{L^{\text{ab}}/L} & & \downarrow & & \downarrow \\
 1 & \longrightarrow & C_L & \longrightarrow & W_{L/\mathbb{Q}} & \longrightarrow & \text{Gal}(L/\mathbb{Q}) \longrightarrow 1
 \end{array}$$

The lower portion of this diagram with maps labeled is the following diagram:

$$\begin{array}{ccccccc}
 & & & & W_L^c/W_{L^{\text{ab}}}^c & & \\
 & & & & \downarrow & & \\
 1 & \longrightarrow & C_{L^{\text{ab}}} & \xrightarrow{r_{L^{\text{ab}}}} & W_{L^{\text{ab}}/\mathbb{Q}} & \xrightarrow{\tilde{\varphi}_{L^{\text{ab}}/\mathbb{Q}}} & \text{Gal}(L^{\text{ab}}/\mathbb{Q}) \longrightarrow 1 \\
 & & \downarrow N_{L^{\text{ab}}/L} & & \downarrow \pi_W & & \downarrow \pi_G \\
 1 & \longrightarrow & C_L & \xrightarrow{r_L} & W_{L/\mathbb{Q}} & \xrightarrow{\tilde{\varphi}_{L/\mathbb{Q}}} & \text{Gal}(L/\mathbb{Q}) \longrightarrow 1
 \end{array}$$

By Artin reciprocity, and noting that $\text{Gal}(L^{\text{ab}}/L)$ is abelian,

$$\text{Gal}(L^{\text{ab}}/L) \cong C_L/N_{L^{\text{ab}}/L}C_{L^{\text{ab}}}$$

Note that the Artin reciprocity map is given by Snake Lemma applied to the diagram above:

$\ker \pi_G \cong \text{Gal}(L^{\text{ab}}/L)$, and $\text{coker } N_{L^{\text{ab}}/L} \cong C_L/N_{L^{\text{ab}}/L}C_{L^{\text{ab}}}$.

$L \leq L^{\text{ab}}$ so $W_{L^{\text{ab}}} \leq W_L$ so $W_{L^{\text{ab}}/\mathbb{Q}}$ surjects onto $W_{L/\mathbb{Q}}$

Also

$$W_{L^{\text{ab}}/L}/(W_L^c/W_{L^{\text{ab}}}^c) \cong W_L^{\text{ab}} \cong C_L$$

$\text{Gal}(L^{\text{ab}}/L) = G_L/G_{L^{\text{ab}}} = W_L/W_{L^{\text{ab}}}$ is abelian.

This means that $(W_L/W_{L^{\text{ab}}})^c = \{1\}$ but that is equivalent to $W_L^c \subset W_{L^{\text{ab}}}$.

Since $[xA, yA] = xAyAx^{-1}Ay^{-1}A = xyx^{-1}y^{-1}((y((x(y^{-1}Ay)x^{-1})A)y^{-1})A) = [x, y]A$

we have $(W_L/W_{L^{\text{ab}}})^c = W_L^c/W_{L^{\text{ab}}}^c$

But then

$$W_L^c/W_{L^{\text{ab}}}^c \leq W_{L^{\text{ab}}}^{\text{ab}} \cong C_{L^{\text{ab}}}$$

Since

$$\ker(\pi : W_{L^{\text{ab}}/\mathbb{Q}} \rightarrow W_{L/\mathbb{Q}}) \leq \ker(\tilde{\varphi} : W_{L^{\text{ab}}/\mathbb{Q}} \rightarrow \text{Gal}(L^{\text{ab}}/\mathbb{Q}))$$

the map $\tilde{\varphi}$ factors as $\pi'\pi$ for some $\pi' : W_{L/\mathbb{Q}} \rightarrow \text{Gal}(L^{\text{ab}}/\mathbb{Q})$.

Furthermore it is clear that this map is surjective.

Let $\pi'(x) = \tilde{\varphi}(\pi^{-1}(x))$ for $\pi' : W_{L/\mathbb{Q}} \rightarrow \text{Gal}(L^{\text{ab}}/\mathbb{Q})$. Since π is surjective (it is a quotient), $\pi^{-1}(x)$ is nonempty. Note if $y_1, y_2 \in \pi^{-1}(x)$, then $y_1 y_2^{-1} \in W_L^c / W_{L^{\text{ab}}}^c \leq W_{L^{\text{ab}}}^{\text{ab}}$, so that $y_1 y_2^{-1} \in \text{im } r_{L^{\text{ab}}}$. But then $\tilde{\varphi}(y_1) = \tilde{\varphi}(y_2)$, so that π' is well-defined. Then note

$$\pi'\pi(x) = \tilde{\varphi}(\pi^{-1}\pi(x)) = \tilde{\varphi}(xW_L^c / W_{L^{\text{ab}}}^c) \leq \tilde{\varphi}(xW_{L^{\text{ab}}}^{\text{ab}}) = \tilde{\varphi}(x \text{im } r_{L^{\text{ab}}}) = \tilde{\varphi}(x)$$

Since π is surjective, this also settles the question of π' being a homomorphism.

On the other hand,

$$\pi'(\pi(\tilde{\varphi}^{-1}(x))) = \tilde{\varphi}(\tilde{\varphi}^{-1}(x)) = x.$$

Note here that $\tilde{\varphi}$ is surjective, therefore $\tilde{\varphi}^{-1}(x)$ is nonempty and contains an element y_0 , and $\tilde{\varphi}^{-1}(x) = y_0 \ker \tilde{\varphi}$.

Thus we have the commutative diagram:

$$\begin{array}{ccccccc} & & W_L^c / W_{L^{\text{ab}}}^c & \xrightarrow{\text{res}(\tilde{\varphi})} & \text{Gal}(L^{\text{ab}}/L) & & \\ & & \downarrow \iota_W & & \downarrow \iota_G & & \\ 1 \longrightarrow & C_{L^{\text{ab}}} & \xrightarrow{r_{L^{\text{ab}}}} & W_{L^{\text{ab}}/\mathbb{Q}} & \xrightarrow{\tilde{\varphi}_{L^{\text{ab}}/\mathbb{Q}}} & \text{Gal}(L^{\text{ab}}/\mathbb{Q}) & \longrightarrow 1 \\ & \downarrow N_{L^{\text{ab}}/L} & & \downarrow \pi_W & \nearrow \pi' & \downarrow \pi_G & \\ 1 \longrightarrow & C_L & \xrightarrow{r_L} & W_{L/\mathbb{Q}} & \xrightarrow{\tilde{\varphi}_{L/\mathbb{Q}}} & \text{Gal}(L/\mathbb{Q}) & \longrightarrow 1 \end{array}$$

Now note

$$\text{im } \pi' r_L \leq \ker \pi_G = \text{im } \iota_G.$$

Since $\pi'\pi_W = \tilde{\varphi}_{L^{\text{ab}}/\mathbb{Q}}$, we have that

$$\pi_G \pi' \pi_W = \pi_G \tilde{\varphi}_{L^{\text{ab}}/\mathbb{Q}} = \tilde{\varphi}_{L/\mathbb{Q}} \pi_W$$

Since π_W is surjective, this implies that

$$\pi_G \pi' = \tilde{\varphi}_{L/\mathbb{Q}}$$

But then we have

$$\pi_G \pi' r_L = \tilde{\varphi}_{L/\mathbb{Q}} r_L = 0$$

Hence $\text{im}(\pi' r_L) \leq \ker(\pi_G) = \text{im}(\iota_G)$.

Therefore there exists a homomorphism $\pi'' : C_L \rightarrow \text{Gal}(L^{\text{ab}}/L)$ such that

$$\iota_G \pi'' = \pi' r_L$$

Note that since ι_G is injective, above equality forces π'' to be a homomorphism.

To see that it is surjective note, if $w \in \tilde{\varphi}_{L^{\text{ab}}/\mathbb{Q}}^{-1}(\iota_G(\sigma))$ for some $\sigma \in \text{Gal}(L^{\text{ab}}/L)$, then $\pi_W(w) \in \text{im}(r_L) = \ker(\tilde{\varphi}_{L/\mathbb{Q}})$.

Since $\tilde{\varphi}_{L/\mathbb{Q}} \pi_W(w) = \pi_G \tilde{\varphi}_{L^{\text{ab}}/\mathbb{Q}}(w) = \pi_G \iota_G(\sigma) = 0$, above holds. But then $r_L^{-1}(\pi_W(\tilde{\varphi}_{L^{\text{ab}}/\mathbb{Q}}^{-1}(\iota_G(\sigma))))$ is nonempty, and if $x \in C_L$ is an element there, then $\pi''(x) = \sigma$.

This gives the commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_L & \xrightarrow{r_L} & W_{L/\mathbb{Q}} & \xrightarrow{\tilde{\varphi}_{L/\mathbb{Q}}} & \text{Gal}(L/\mathbb{Q}) & \longrightarrow & 1 \\ & & \downarrow \pi'' & & \downarrow \pi' & & \downarrow \text{id} & & \\ 1 & \longrightarrow & \text{Gal}(L^{\text{ab}}/L) & \xrightarrow{\iota_G} & \text{Gal}(L^{\text{ab}}/\mathbb{Q}) & \xrightarrow{\pi_G} & \text{Gal}(L/\mathbb{Q}) & \longrightarrow & 1 \end{array}$$

Note that π'' is the norm-residue map.

7.7. LEMMAS FOR NUMBER THEORETIC BACKGROUND

Lemma 73 *If $f : G \rightarrow H$ is a group homomorphism with $G_0 = f^{-1}(H_0)$ for a subgroup H_0 of H , then f induces a morphism $\tilde{f} : G/G_0 \rightarrow H/H_0$ which is a group homomorphism if H_0 is normal in H . Furthermore if $G_1 = f^{-1}(H_1)$ for H_1 a subgroup of H_0 , then f induces a morphism $\tilde{f} : G_0/G_1 \rightarrow H_0/H_1$. This may be repeated if $G_0 \leq f^{-1}(H_0)$.*

For the first part, define $\tilde{f}(gG_0) = f(g)H_0$. To see well-definedness if g and g' belong to the same G_0 -coset, then $f(g)$ and $f(g')$ belong to the same H_0 -coset, because $f(G_0) \leq H_0$ by definition. To see that this defines a homomorphism when H_0 is normal, note $\tilde{f}(g_1G_0g_2G_0) = \tilde{f}(g_1g_2G_0) = f(g_1g_2)H_0 = f(g_1)f(g_2)H_0 = f(g_1)H_0f(g_2)H_0 = \tilde{f}(g_1G_0)\tilde{f}(g_2G_0)$

For second part, this is repeating the lemma with $\tilde{f} : G/G_1 \rightarrow H/H_1$ on subgroups G_0/G_1 and H_0/H_1 .

Remark Fill in the proof of last modification.

Lemma 74 *If $\iota : A \rightarrow B$ is group homomorphism (and most likely an injection), and A_0 is a (normal) subgroup of A that is mapped into B_0 , then we have the commutative diagram:*

$$\begin{array}{ccccccc}
 A/A_0 & \longrightarrow & B/B_0 & \longrightarrow & (B/B_0)/(A/A_0) & \cong & (B/A)/(B_0/A_0) \\
 \uparrow & & \uparrow & & \uparrow & & \uparrow \\
 A & \longrightarrow & B & \longrightarrow & B/A & & \\
 \uparrow & & \uparrow & & \uparrow & & \uparrow \\
 A_0 & \longrightarrow & B_0 & \longrightarrow & B_0/A_0 & &
 \end{array}$$

Remark Fill in details, and check for errors.

Lemma 75 *If $\iota : H \rightarrow G$ is inclusion of groups, there is a group homomorphism $G/H \rightarrow G^{\text{ab}}/H^{\text{ab}}$*

Apply previous lemma. **Remark** Fill in the proof of this statement. In fact characterize $(G/H)^{\text{ab}}$.

Lemma 76 *If A , and B are topological groups, with $\varphi : A \rightarrow B$ a topological group homomorphism, i.e. a continuous group homomorphism, and $\varphi(A)$ is dense in B , and B_0 is an open subgroup of B , (of finite index) and $A_0 = \varphi^{-1}(B_0)$, then*

- $\varphi(A_0)$ is dense in B_0 .
- φ induces a continuous map $\tilde{\varphi} : A/A_0 \rightarrow B/B_0$, which is a bijection.
- If B_0 is normal in B , then the continuous map is a group isomorphism.
- If B_1 is a subgroup of B containing B_0 , (i.e. $B \geq B_1 \geq B_0$) and $A_1 = \varphi^{-1}(B_1)$, then $\tilde{\varphi}(A_1/A_0) = B_1/B_0$. Furthermore $\tilde{\varphi}_{A_1, B_1} : A_1/A_0 \rightarrow B_1/B_0$ is also a bijection, and continuous and group isomorphism when B_0 is normal in B .

We start with the diagram:

$$\begin{array}{ccc} & B_0 & \\ & \downarrow \iota_B & \\ A & \xrightarrow{\varphi} & B \end{array}$$

and end up with the diagram

$$\begin{array}{ccc} A_0 & \xrightarrow{\varphi|_{A_0, B_0}} & B_0 \\ \downarrow \iota_A & & \downarrow \iota_B \\ A & \xrightarrow{\varphi} & B \\ \downarrow \pi_A & \searrow \pi_B \circ \varphi & \downarrow \pi_B \\ A/A_0 & \xrightarrow{\tilde{\varphi}} & B/B_0 \end{array}$$

Take an arbitrary point $b \in B_0$, and a neighborhood V of b in B_0 . Since $\varphi(A)$ is dense in B , $V \cap \varphi(A)$ is nonempty, so there exists $a \in A$, such that $\varphi(a) \in V$. But since $V \subseteq B_0$, so that $a \in \varphi^{-1}(B_0) = A_0$.

$\pi_B \circ \varphi$ is a continuous map (and a group homomorphism when B_0 is normal), whose kernel contains $A_0 = \varphi^{-1}(B_0)$, because $B_0 = \ker \pi_B$. Therefore $\pi_B \circ \varphi$ factorizes through π_A . When normality fails, $\tilde{\varphi}(aA_0) = \varphi(a)B_0$ is a well-defined map, since $\varphi(A_0) \subseteq B_0$. i.e. If a, a' lie in same A_0 -coset, then $\varphi(a)$ and $\varphi(a')$ lie in same B_0 -coset.

On the other hand, the definition of quotient topology makes $\tilde{\varphi}$ continuous.

If $\tilde{\varphi}(aA_0) = \tilde{\varphi}(a'A_0)$, then $\varphi(a)B_0 = \varphi(a')B_0$ by definition of $\tilde{\varphi}$. But then $\varphi(a)$ and $\varphi(a')$ lie in same B_0 -coset, so that $\varphi(a^{-1}a') \in B_0$, i.e. $a^{-1}a' \in A_0 = \varphi^{-1}(B_0)$. Hence $aA_0 = a'A_0$. This proves injectivity.

If $b \in B$, is arbitrary, Since $\varphi(A)$ is dense in B , then $\varphi(A) \cap bB_0$ is nonempty, i.e. there exists $a \in A$ such that $\varphi(a) \in bB_0$, i.e. $b^{-1}\varphi(a) \in B_0$. But $\varphi(A_0)$ is dense in B_0 , so any neighborhood V of $b^{-1}\varphi(a)$ in B_0 contains an element of $\varphi(A_0)$. in other words there exists $a_0 \in A_0$, such that $\varphi(a_0) \in V \subseteq B_0$. But then $b^{-1}\varphi(a)\varphi(a_0) \in B_0$, since B_0 is a subgroup. Then we have $\varphi(aa_0) = bB_0$, so that $\tilde{\varphi}(aA_0) = \varphi(aa_0)B_0 = bB_0$. This establishes surjectivity.

If B_0 is normal in B , then A_0 is normal in A , since $\varphi(xax^{-1}) = \varphi(x)\varphi(a)\varphi(x)^{-1}$. For

$x \in A$ and $a \in A_0$, note $\varphi(a) \in \varphi(A_0) \leq B_0$, and $A_0 = \varphi^{-1}(B_0)$.

$\tilde{\varphi}(a_1 B_0 a_2 B_0) = \tilde{\varphi}(a_1 a_2 A_0) = \varphi(a_1 a_2) B_0 = \varphi(a_1) B_0 \varphi(a_2) B_0 = \tilde{\varphi}(a_1 A_0) \tilde{\varphi}(a_2 A_0)$ This establishes that $\tilde{\varphi}$ is a group homomorphism.

A group homomorphism which is a set bijection is automatically a group isomorphism.

Now start with the diagram:

$$\begin{array}{ccc} A_0 & \xrightarrow{\varphi_0} & B_0 \\ \downarrow \iota & & \downarrow \iota \\ A_1 & \xrightarrow{\varphi_1} & B_1 \\ \downarrow \iota & & \downarrow \iota \\ A & \xrightarrow{\varphi} & B \end{array}$$

and end up with the diagram:

$$\begin{array}{ccc} 1 & & 1 \\ \downarrow & & \downarrow \\ A_1/A_0 & \xrightarrow{\tilde{\varphi}_{1,0}} & B_1/B_0 \\ \downarrow \iota & & \downarrow \iota \\ A/A_0 & \xrightarrow{\tilde{\varphi}_0} & B/B_0 \\ \downarrow \pi & & \downarrow \pi \\ A/A_1 & \xrightarrow{\tilde{\varphi}_1} & B/B_1 \\ \downarrow & & \downarrow \\ 1 & & 1 \end{array}$$

Isomorphisms (or bijections when respective subgroups are not normal) $\tilde{\varphi}_i : A/A_i \rightarrow B/B_i$ for $i = 0, 1$ come from the first part of the lemma. They form a commutative diagram with projections by their definition.

$\tilde{\varphi}_0(A_1/A_0) = \Pi_{a \in A_1} \varphi(a) B_0 \leq B_1/B_0$. Therefore the map (homomorphism, when subgroups are normal) $\tilde{\varphi}_{1,0} : A_1/A_0 \rightarrow B_1/B_0$ is defined and forms a commutative diagram with injections $\iota : A_1/A_0 \rightarrow A/A_0$ and $\iota : B_1/B_0 \rightarrow B/B_0$. $\tilde{\varphi}_{1,0}$ is injective, because it is obtained by restricting an injection.

On the other hand given an arbitrary element $b_1 \in B_1$, since $\varphi(A_1)$ is dense in B_1 , the neighborhood $b_1 B_0$ of b_1 contains an element in $\varphi(A_1)$, say $\varphi(a_1)$. Then $\tilde{\varphi}_{1,0}(a_1 A_0) = \varphi(a_1) B_0 = b_1 B_0$. This proves that $\tilde{\varphi}_{1,0}$ is also surjective, i.e. is an isomorphism. Hence all

the horizontal maps above in the diagram are bijections, and if B_0 and B_1 are normal in B , then they are group isomorphisms.

7.8. TRANSFER MAP

Let G be a topological group, and H a closed subgroup of finite index, and $s_i : H \backslash G \rightarrow G$, for $i = 1, 2$ two sections of cosets, for $\pi : G \rightarrow H \backslash G$, being the projection to the coset space, so that $\pi \circ s_i = \text{id}$. Let

$$t'_i(g) = \prod_{x \in H \backslash G} s_i(x) g s_i(xg)^{-1}$$

Let $\pi^{\text{ab}} : H \rightarrow H^{\text{ab}} = H/[H, H]$, be the abelianization map.

Now define

$$t_i(g) = \pi^{\text{ab}}(t'_i(g))$$

Since $\pi(s_i(xg)) = xg = \pi(s_i(x))g = \pi(s_i(x)g)$ we have that $s_i(x)g$ and $s_i(xg)$ lie in the same H -coset. (Note $(Hb)g = H(bg)$. This is the action of G from the right on right cosets of H in G .) Therefore $s_i(x)g s_i(xg)^{-1} \in H$.

Let $v_i(x, g) = s_i(x)g s_i(xg)^{-1} \in H$.

Now we have

$$\begin{aligned} t_1(g)t_2(g)^{-1} &= \pi^{\text{ab}} \left(\prod_{x \in H \backslash G} v_1(x, g) \right) \pi^{\text{ab}} \left(\prod_{x \in H \backslash G} v_2(x, g) \right)^{-1} \\ &= \pi^{\text{ab}} \left(\prod_{x \in H \backslash G} v_1(x, g) v_2(x, g)^{-1} \right) \end{aligned}$$

where we utilize the fact that π^{ab} is a homomorphism, and H^{ab} is an abelian group, to rearrange the order of the terms.

Let $u(x) = s_2(x)s_1(x)^{-1} \in H$, then $u(x)s_1(x) = s_2(x)$, and

Then we have

$$\begin{aligned}
 v_2(x, g) &= s_2(x)gs_2(xg)^{-1} \\
 &= u(x)s_1(x)g(u(xg)s_1(xg))^{-1} \\
 &= u(x)s_1(x)gs_1(xg)^{-1}u(xg)^{-1} \\
 &= u(x)v_1(x, g)u(xg)^{-1}
 \end{aligned}$$

So that

$$\begin{aligned}
 v_1(x, g)v_2(x, g)^{-1} &= v_1(x, g)(u(x)v_1(x, g)u(xg)^{-1})^{-1} \\
 &= v_1(x, g)u(xg)v_1(x, g)^{-1}u(x)^{-1} \\
 &= v_1(x, g)u(xg)v_1(x, g)^{-1}u(xg)^{-1}u(xg)u(x)^{-1} \\
 &= [v_1(x, g), u(xg)]u(xg)u(x)^{-1}
 \end{aligned}$$

But then we have:

$$\begin{aligned}
t_1(g)t_2(g)^{-1} &= \pi^{\text{ab}} \left(\prod_{x \in H \setminus G} [v_1(x, g), u(xg)] u(xg) u(x)^{-1} \right) \\
&= \pi^{\text{ab}} \left(\prod_{x \in H \setminus G} u(xg) u(x)^{-1} \right) \\
&= \pi^{\text{ab}} \left(\prod_{x \in H \setminus G} u(xg) \right) \pi^{\text{ab}} \left(\prod_{x \in H \setminus G} u(x)^{-1} \right) \\
&= \pi^{\text{ab}} \left(\prod_{x \in H \setminus G} u(x) \right) \pi^{\text{ab}} \left(\prod_{x \in H \setminus G} u(x)^{-1} \right) \\
&= 1
\end{aligned}$$

This shows that $t : G \rightarrow H^{\text{ab}}$ is independent of choice of section $s : H \setminus G \rightarrow G$.

Now consider the following:

$$\begin{aligned}
&t(g)t(h) \\
&= \pi^{\text{ab}} \left(\prod_{x \in H \setminus G} s(x)gs(xg)^{-1} \right) \pi^{\text{ab}} \left(\prod_{x \in H \setminus G} s(x)hs(xh)^{-1} \right) \\
&= \pi^{\text{ab}} \left(\prod_{x \in H \setminus G} s(x)gs(xg)^{-1} \right) \pi^{\text{ab}} \left(\prod_{x \in H \setminus G} s(xg)hs(xgh)^{-1} \right) \\
&= \pi^{\text{ab}} \left(\prod_{x \in H \setminus G} s(x)gs(xg)^{-1}s(xg)hs(xgh)^{-1} \right) \\
&= \pi^{\text{ab}} \left(\prod_{x \in H \setminus G} s(x)ghs(xgh)^{-1} \right) \\
&= t(gh)
\end{aligned}$$

Therefore $t(g)t(h) = t(gh)$, proving that t is a homomorphism. Since H^{ab} is abelian, the map factors through the abelianization of G , yielding $\text{tr} : G^{\text{ab}} \rightarrow H^{\text{ab}}$.

Note that we can break down the factorization:

$$G \rightarrow G/[G, G] \rightarrow G/\overline{[G, G]}.$$

There is a minor topological consideration in completing the full transfer map.

$$\begin{array}{ccc} G & \xrightarrow{t'} & H \\ \downarrow & \searrow t & \downarrow \\ G/[G, G] & \longrightarrow & H/[H, H] \\ \downarrow & & \downarrow \\ G/\overline{[G, G]} & \dashrightarrow & H/\overline{[H, H]} \end{array}$$

The triangle

$$\begin{array}{ccc} G & & \\ \downarrow & \searrow t & \\ G/[G, G] & \longrightarrow & H/[H, H] \end{array}$$

out.

is algebraic, and is due to the computations carried

It suffices to claim that the middle map carries the closure of $[G, G]$ into the closure of $[H, H]$.

One possible direction of argument is the following: $[G, G]$ is the image of a continuous map, defined by group operations. We also note that since $H \setminus G$ the coset space is a finite set, and H is closed, (hence open), it has discrete topology, hence the section is automatically continuous, which makes the transfer map before passing to the final quotient, continuous, i.e. t' is continuous but not necessarily a homomorphism. Therefore t is continuous and a homomorphism.

We note that we have the following topological lemma.

Lemma 77 *If $f : A \rightarrow B$ is continuous, then $f(\overline{A_0}) \subseteq \overline{f(A_0)}$.*

Note that $f^{-1}(\overline{f(A_0)})$ is a closed set containing A_0 , hence must contain $\overline{A_0}$.

Theorem 19 *If H is normal in G , then the composition $H^{\text{ab}} \xrightarrow{\iota} G^{\text{ab}} \xrightarrow{\text{tr}} H^{\text{ab}}$ takes h*

into the product of its conjugates by representatives of elements of G/H , where ι is induced by inclusion.

Note

$$\begin{aligned} t(h) &= \pi^{\text{ab}} \prod_{x \in G/H} s(x) h s(xh)^{-1} \\ &= \pi^{\text{ab}} \prod_{x \in G/H} s(x) h s(x)^{-1} s(x) s(xh)^{-1} \end{aligned}$$

But $s(x)$ and $s(xh)$ lie in the same coset. ($Hbh = Hbhb^{-1}b = Hb$.) Therefore

$$t(h) = \pi^{\text{ab}} \prod_{x \in G/H} s(x) h s(x)^{-1}$$

Lemma 78 Every group homomorphism f from a group G to an abelian group A factorizes through the abelianization of the source group, G^{ab} .

$$\begin{array}{ccc} G & \xrightarrow{f} & A \\ \pi^{\text{ab}} \downarrow & \nearrow \tilde{f} & \\ G^{\text{ab}} = G/G^c & & \end{array}$$

Define $\tilde{f}(xG^c) = f(x)$. Note that for $a, b \in G$, we have

$$f(x[a, b]) = f(x)f([a, b]) = f(x)[f(a), f(b)] = f(x)$$

This shows that $\tilde{f} : G/[G, G] \rightarrow A$ is well-defined. Since

$$\tilde{f}(xG^c yG^c) = \tilde{f}(xyG^c) = f(xy) = f(x)f(y) = \tilde{f}(xG^c)\tilde{f}(yG^c)$$

it is a group homomorphism, for $G^c = [G, G]$.

Note $[G, G] \leq \ker f$. If f is continuous, and $\{0\}$ is closed in A , then $\overline{[G, G]} \leq \ker f$. This also establishes continuity of $\tilde{f} : G/G^c \rightarrow A$.

Lemma 79 Every group homomorphism from an abelian group into a group has an abelian image.

If $f : A \rightarrow G$ is a group homomorphism, with A abelian, then

$$f(x)f(y) = f(xy) = f(yx) = f(y)f(x).$$

Hence $f(A)$ is abelian.

Lemma 80 *If $f : G \rightarrow H$ is a group homomorphism, this induces a group homomorphism $f^{\text{ab}} : G^{\text{ab}} \rightarrow H^{\text{ab}}$.*

First note:

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ & \searrow \pi^{\text{ab}} \circ f & \downarrow \pi^{\text{ab}} \\ & & H^{\text{ab}} \end{array}$$

is just composition of the homomorphisms. By previous lemma, $\pi^{\text{ab}} \circ f$ factorizes through the abelianization of G :

$$\begin{array}{ccc} G & & \\ \pi_G^{\text{ab}} \downarrow & \searrow \pi_H^{\text{ab}} \circ f & \\ G^{\text{ab}} & \xrightarrow{f^{\text{ab}}} & H^{\text{ab}} \end{array}$$

Lemma 81 A^c is normal in A .

Note

$$g[x, y]g^{-1} = [g, [x, y]][x, y]$$

Lemma 82 *If A is normal in B , then A^c is normal in B .*

Note

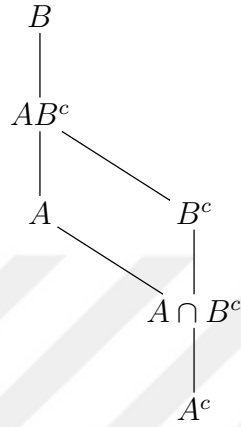
$$g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$$

Lemma 83 *If A is normal in B , then*

$$(B/A)^c = B^c A/A = B^c/(B^c \cap A)$$

and so

$$(B/A)^{\text{ab}} \cong (B/B^c)/((A/A^c)/((A \cap B^c)/A^c)) \cong B^{\text{ab}}/\iota^{\text{ab}}(A^{\text{ab}}) \cong B^{\text{ab}}/(\iota(A))^{\text{ab}}$$



Now let $\pi : B^c \rightarrow (B/A)^c$ be the surjective homomorphism defined by

$$\pi([x, y]) = [xA, yA] = [x, y]A.$$

Note:

$$\begin{aligned}
 [xA, yA] &= xAyAx^{-1}Ay^{-1}A \\
 &= xy(y^{-1}Ay)Ax^{-1}Ay^{-1}A \\
 &= xyAx^{-1}Ay^{-1}A \\
 &= xyx^{-1}(xAx^{-1})Ay^{-1}A \\
 &= xyx^{-1}Ay^{-1}A \\
 &= xyx^{-1}y^{-1}(yAy^{-1})A
 \end{aligned}$$

$$= xyx^{-1}y^{-1}A$$

$$= [x, y]A$$

Now $\text{Ker}\pi = B^c \cap A$. So that $B^c/(B^c \cap A) \cong (B/A)^c$. Now

$$(B/A)^{\text{ab}} = (B/A)/(B/A)^c$$

$$= (B/A)/(B^c A/A)$$

$$= B/(B^c A)$$

$$= (B/B^c)/(B^c A/B^c)$$

$$= (B/B^c)/(A/(A \cap B^c))$$

$$= (B/B^c)/((A/A^c)/((A \cap B^c)/A^c))$$

If $\iota : A \rightarrow B$ denotes the inclusion, then $\iota^{\text{ab}} : A^{\text{ab}} \rightarrow B^{\text{ab}}$ has kernel $A \cap B^c/A^c$.

Note

$$\begin{array}{ccccc}
 A \cap B^c & \xleftarrow{\quad} & A^c & \xrightarrow{\quad} & B^c \\
 \downarrow & \searrow & \downarrow & & \downarrow \\
 & & A & \xrightarrow{\quad \iota \quad} & B \\
 & & \downarrow & \searrow \tilde{\iota} & \downarrow \\
 A \cap B^c/A^c & \longrightarrow & A^{\text{ab}} & \xrightarrow{\quad \iota^{\text{ab}} \quad} & B^{\text{ab}}
 \end{array}$$

Here

$$\text{Ker } \tilde{\iota} = A \cap B^c = \iota^{-1}(\iota(A) \cap B^c)$$

Hence

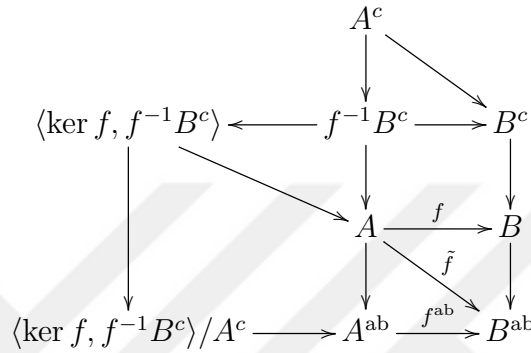
$$\text{Ker } \iota^{\text{ab}} = A \cap B^c/A^c.$$

So then :

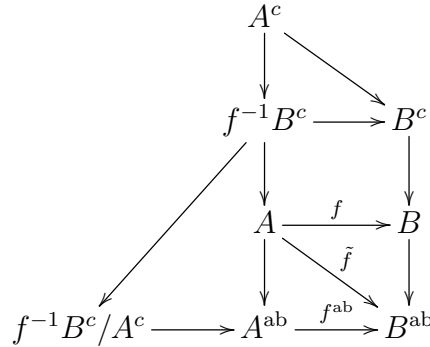
$$(B/A)^{\text{ab}} \cong (B/B^c)/((A/A^c)/((A \cap B^c)/A^c)) \cong B^{\text{ab}}/\iota^{\text{ab}}(A^{\text{ab}}) \cong B^{\text{ab}}/(\iota(A))^{\text{ab}}$$

Let's try to generalize the above for a group homomorphism $f : A \rightarrow B$ instead of inclusion.

Note



Though note $\ker f \leq f^{-1}B^c$, so that $\langle \ker f, f^{-1}B^c \rangle = f^{-1}B^c$ but we keep it in the diagram in order to keep in mind that $\ker f \leq \ker \tilde{f}$. So we can redraw the diagram as follows:



Lemma 84 If $f : A \rightarrow B$ is a group homomorphism, then $\ker f^{\text{ab}} \cong f^{-1}B^c/A^c$, and $\text{im } f^{\text{ab}} \cong \text{im } f / \text{im } f \cap B^c$.

Lemma 85 If $f : A \rightarrow B$ is a surjective group homomorphism, then so is $f^{\text{ab}} : A^{\text{ab}} \rightarrow B^{\text{ab}}$.

Note that $\tilde{f} = \pi_B^{\text{ab}} \circ f$, being a composition of surjective maps, is surjective. But $\tilde{f} = f^{\text{ab}} \circ \pi_A^{\text{ab}}$ where $\tilde{f}$ and π_A^{ab} are both surjective. Then f^{ab} has to be surjective.

Lemma 86

$$\begin{array}{ccccc}
A & \xrightarrow{f} & B & \xrightarrow{g} & C \\
\downarrow & & \downarrow & & \downarrow \\
A^{\text{ab}} & \xrightarrow{f^{\text{ab}}} & B^{\text{ab}} & \xrightarrow{g^{\text{ab}}} & C^{\text{ab}}
\end{array}$$

If $\text{im } f \leq \ker g$ then $\text{im } f^{\text{ab}} \leq \ker g^{\text{ab}}$

By previous lemma, we have $\text{im } f^{\text{ab}} \cong \text{im } f / \text{im } f \cap B^c \cong \text{im } f B^c / B^c$

By assumption, $\text{im } f^{\text{ab}} \cong \text{im } f B^c / B^c \leq \ker g B^c / B^c$.

On the other hand, again by previous lemma we have $\ker g^{\text{ab}} \cong g^{-1} C^c / B^c$,

It is evident that $\text{im } f^{\text{ab}} \leq \ker g^{\text{ab}}$.

Since $B^c \leq g^{-1} C^c$, or $g(B^c) = g(B)^c \leq C^c$.

7.9. SEMIDIRECT PRODUCTS

We will discuss if the a group can be written as a semidirect product with one of its normal subgroups and the quotient of the group by this normal subgroup. If $N \trianglelefteq G$, is $G = H \ltimes N = N \rtimes H$, where $H \cong G/N$, acts by inner conjugation on N ?

First of all let's discuss if the action of G/N on N by inner conjugation is well defined. If $y = xm$, where $m \in N$, then we have $yn y^{-1} = xmn(xm)^{-1} = xmn m^{-1} x^{-1} = xmx^{-1}(xnx^{-1})xm^{-1}x^{-1}$, for $m, n \in N$. On the other hand, if $y = mx$, then $yn y^{-1} = (mx)n(mx)^{-1} = m(xnx^{-1})m^{-1}$. So changing coset representatives will change the action on N by inner conjugation in N . However if N is abelian, then N 's action on itself by inner conjugation is trivial, hence the action of G/N on N by inner conjugation can be defined.

On the set $G/N \times N$ let's try to define an operation by

$$(x, m) \circ (y, n) = (xy, m^{y^{-1}} n)$$

where $m^{y^{-1}}$ denotes $y^{-1} \in G/N$ acting on $m \in N$, assuming such an action is known.

Then we have, suppressing usage of the group operation $\circ$ defined above,

$$((x, m)(y, n))(z, k) = (xy, m^{(y^{-1})} n)(z, k) = (xyz, (m^{(y^{-1})} n)^{(z^{-1})} k) = (xyz, (m^{(y^{-1})})^{(z^{-1})} n^{(z^{-1})} k)$$

$$(x, m)((y, n)(z, k)) = (x, m)(yz, n^{(z^{-1})} k) = (xyz, m^{((yz)^{-1})} n^{(z^{-1})} k)$$

But note $(m^y)^z = m^{zy}$. So that associativity holds.

Note that $(1, 1)$ is identity of this operation, and $(x^{-1}, (m^x)^{-1}) = (x^{-1}, (m^{-1})^x)$ is inverse of (x, m) .

For a section $s : G/N \rightarrow G$ of $\pi : G \rightarrow G/N$, one way in which G/N could act on N is by inner conjugation: $m^x = s(x)ms(x)^{-1}$. However as stated above there is a problem with this choice, because this is not guaranteed to define a group action, unless N is abelian.

If there is a section $s : G/N \rightarrow G$ that is a group homomorphism, then one can establish that G is isomorphic to $(G/N \times N, \circ)$ with the group operation as defined above, with the group isomorphism $\rho : (G/N \times N, \circ) \rightarrow G$ being given by $(x, m) \mapsto s(x)m$. In order to see that this is a group homomorphism, note:

$$\begin{aligned}
 \rho((x, m) \circ (y, n)) &= \rho((xy, m^{y^{-1}}n)) \\
 &= s(xy)m^{y^{-1}}n \\
 &= s(x)s(y)s(y)^{-1}ms(y)n \\
 &= s(x)ms(y)n \\
 &= \rho((x, m))\rho((y, n)).
 \end{aligned}$$

By changing the order of representation, one obtains another way of forming group G from N and G/N . Let the group operation on the set $N \times G/N$ be defined by:

$$(m, x)(n, y) = (mn^x, xy).$$

Suppose $G = HN$, for some $H \leq G$ so that each element is representable as hn with $h \in H$, and $n \in N$. (In fact, we can instead just work on HN , even when $HN \leq G$, when N is just some subgroup, and $H \leq N_G(N)$, i.e. H lies in the normalizer of N in G , those

elements of G where inner conjugation maps the group to itself.) Then

$$h_1 n_1 h_2 n_2 = h_1 h_2 (h_2^{-1} n_1 h_2) n_2$$

Alternatively if the representation is chosen as nh , then

$$n_1 h_1 n_2 h_2 = n_1 (h_1 n_2 h_1^{-1}) h_1 h_2$$

Now if N is abelian, then action of G/N on N can be defined independent of the section chosen.

If $\varphi : G/N \rightarrow \text{Aut}(N)$ is a homomorphism, then semidirect product can be defined, via this homomorphism.

If the section can be chosen to be an injective homomorphism, then $H \leq G$ exists such that $HN = G$.

Rewrite - Semidirect Products

If $\varphi : H \rightarrow \text{Aut}(N)$, is a group homomorphism, then the set $N \times H$ acquires a group structure by defining:

$$(n_1, h_1)(n_2, h_2) = (n_1 \varphi(h_1)(n_2), h_1 h_2)$$

(Alternatively, on $H \times N$ by

$$(h_1, n_1)(h_2, n_2) = (h_1 h_2, \varphi(h_2^{-1})(n_1) n_2)$$

This is modeled after the case when H is a subgroup of G such that $G = HN = NH$, where H acts on G by inner conjugation.

Associativity:

$$\begin{aligned}
 ((n_1, h_1)(n_2, h_2))(n_3, h_3) &= (n_1\varphi(h_1)(n_2), h_1h_2)(n_3, h_3) \\
 &= ((n_1\varphi(h_1)(n_2))\varphi(h_1h_2)(n_3), (h_1h_2)h_3) \\
 &= ((n_1\varphi(h_1)(n_2))(\varphi(h_1)\varphi(h_2))(n_3), (h_1h_2)h_3) \\
 &= ((n_1\varphi(h_1)(n_2))(\varphi(h_1)(\varphi(h_2)(n_3))), h_1h_2h_3)
 \end{aligned}$$

$$\begin{aligned}
 (n_1, h_1)((n_2, h_2)(n_3, h_3)) &= (n_1, h_1)(n_2\varphi(h_2)(n_3), h_2h_3) \\
 &= (n_1\varphi(h_1)(n_2\varphi(h_2)(n_3)), h_1(h_2h_3)) \\
 &= (n_1\varphi(h_1)(n_2)\varphi(h_1)(\varphi(h_2)(n_3)), h_1h_2h_3)
 \end{aligned}$$

Associativity - alternate

$$\begin{aligned}
 ((h_1, n_1)(h_2, n_2))(h_3, n_3) &= (h_1h_2, \varphi(h_2^{-1})(n_1)n_2)(h_3, n_3) \\
 &= ((h_1h_2)h_3, (\varphi(h_3^{-1})(\varphi(h_2^{-1})(n_1)n_2))n_3) \\
 &= ((h_1h_2)h_3, \varphi(h_3^{-1})(\varphi(h_2^{-1})(n_1))\varphi(h_3^{-1})(n_2)n_3)
 \end{aligned}$$

$$\begin{aligned}
(h_1, n_1)((h_2, n_2)(h_3, n_3)) &= (h_1, n_1)(h_2 h_3, \varphi(h_3^{-1})(n_2) n_3) \\
&= (h_1(h_2 h_3), \varphi((h_2 h_3)^{-1})(n_1) \varphi(h_3^{-1})(n_2) n_3) \\
&= (h_1(h_2 h_3), \varphi(h_3^{-1} h_2^{-1})(n_1) \varphi(h_3^{-1})(n_2) n_3) \\
&= (h_1(h_2 h_3), (\varphi(h_3^{-1}) \varphi(h_2^{-1}))(n_1) \varphi(h_3^{-1})(n_2) n_3) \\
&= (h_1 h_2 h_3, \varphi(h_3^{-1})(\varphi(h_2^{-1})(n_1)) \varphi(h_3^{-1})(n_2) n_3)
\end{aligned}$$

Unit:

$$\begin{aligned}
(1, 1)(n, h) &= (1\varphi(1)(n), 1h) \\
&= (n, h)
\end{aligned}$$

$$\begin{aligned}
(n, h)(1, 1) &= (n\varphi(h)(1), h1) \\
&= (n, h)
\end{aligned}$$

Unit-alternate:

$$\begin{aligned}
(1, 1)(h, n) &= (1h, \varphi(h^{-1})(1)n) \\
&= (h, n)
\end{aligned}$$

$$\begin{aligned}
 (h, n)(1, 1) &= (h1, \varphi(1^{-1})(n)1) \\
 &= (h, n)
 \end{aligned}$$

Inverse: In the equation

$$(n_1, h_1)(n_2, h_2) = (n_1\varphi(h_1)(n_2), h_1h_2) = (1, 1)$$

Solving for (n_1, h_1) in terms of n_2 and h_2 gives:

$$n_1 = \varphi(h_1)(n_2)^{-1} \text{ and } h_1 = h_2^{-1}, \text{ so } n_1 = \varphi(h_2^{-1})(n_2)^{-1} = \varphi(h_2^{-1})(n_2^{-1}).$$

Solving for (n_2, h_2) in terms of n_1 and h_1 gives:

$$\varphi(h_1)(n_2) = n_1^{-1} \text{ and } h_2 = h_1^{-1} \text{ so } n_2 = \varphi(h_1)^{-1}(n_1^{-1}) = \varphi(h_1^{-1})(n_1^{-1}).$$

Since the two agree, we have:

$$(n, h)^{-1} = (\varphi(h^{-1})(n^{-1}), h^{-1}).$$

Inverse-alternate:

In the equation

$$(h_1, n_1)(h_2, n_2) = (h_1h_2, \varphi(h_2^{-1})(n_1)n_2) = (1, 1)$$

Solving for (h_1, n_1) (in terms of n_2 and h_2) gives:

$$h_1 = h_2^{-1} \text{ and } \varphi(h_2^{-1})(n_1) = n_2^{-1} \text{ so } n_1 = \varphi(h_2^{-1})^{-1}(n_2^{-1}) = \varphi(h_2)(n_2^{-1}).$$

Solving for (h_2, n_2) (in terms of n_1 and h_1) gives:

$$h_2 = h_1^{-1} \text{ and } n_2 = (\varphi(h_2^{-1})(n_1))^{-1} = (\varphi(h_1)(n_1))^{-1} = \varphi(h_1)(n_1^{-1}).$$

Since the two agree, we have

$$(h, n)^{-1} = (h^{-1}, \varphi(h)(n^{-1})).$$

Remark Are other alternatives possible? Are the two semidirect products equivalent in

some sense?

Conjugation in Semidirect Product

$$\begin{aligned}
 (n_1, h_1)(n_2, h_2)(n_1, h_1)^{-1} &= (n_1\varphi(h_1)(n_2), h_1h_2)(\varphi(h_1^{-1})(n_1^{-1}), h_1^{-1}) \\
 &= ((n_1\varphi(h_1)(n_2))\varphi(h_1h_2)(\varphi(h_1^{-1})(n_1^{-1})), h_1h_2h_1^{-1}) \\
 &= (n_1\varphi(h_1)(n_2)\varphi(h_1h_2h_1^{-1})(n_1^{-1}), h_1h_2h_1^{-1})
 \end{aligned}$$

For double-checking in different order:

$$\begin{aligned}
 (n_1, h_1)((n_2, h_2)(n_1, h_1)^{-1}) &= (n_1, h_1)((n_2, h_2)(\varphi(h_1^{-1})(n_1^{-1}), h_1^{-1})) \\
 &= (n_1, h_1)(n_2\varphi(h_2)(\varphi(h_1^{-1})(n_1^{-1})), h_2h_1^{-1}) \\
 &= (n_1, h_1)(n_2\varphi(h_2h_1^{-1})(n_1^{-1})), h_2h_1^{-1}) \\
 &= (n_1\varphi(h_1)(n_2\varphi(h_2h_1^{-1})(n_1^{-1})), h_1h_2h_1^{-1}) \\
 &= (n_1\varphi(h_1)(n_2)\varphi(h_1h_2h_1^{-1})(n_1^{-1}), h_1h_2h_1^{-1})
 \end{aligned}$$

Alternate-form:

$$\begin{aligned}
(h_1, n_1)(h_2, n_2)(h_1, n_1)^{-1} &= (h_1 h_2, \varphi(h_2^{-1})(n_1) n_2)(h_1^{-1}, \varphi(h_1)(n_1^{-1})) \\
&= (h_1 h_2 h_1^{-1}, \varphi((h_1^{-1})^{-1})(\varphi(h_2^{-1})(n_1) n_2)(\varphi(h_1)(n_1^{-1}))) \\
&= (h_1 h_2 h_1^{-1}, \varphi(h_1)(\varphi(h_2^{-1})(n_1) n_2)(\varphi(h_1)(n_1^{-1}))) \\
&= (h_1 h_2 h_1^{-1}, \varphi(h_1)(\varphi(h_2^{-1})(n_1)) \varphi(h_1)(n_2)(\varphi(h_1)(n_1^{-1}))) \\
&= (h_1 h_2 h_1^{-1}, \varphi(h_1)(\varphi(h_2^{-1})(n_1) n_2)(\varphi(h_1)(n_1^{-1}))) \\
&= (h_1 h_2 h_1^{-1}, \varphi(h_1 h_2^{-1})(n_1) \varphi(h_1)(n_2 n_1^{-1}))
\end{aligned}$$

For double-checking in different order:

$$\begin{aligned}
(h_1, n_1)(h_2, n_2)(h_1, n_1)^{-1} &= (h_1, n_1)((h_2, n_2)(h_1^{-1}, \varphi(h_1)(n_1^{-1}))) \\
&= (h_1, n_1)(h_2 h_1^{-1}, \varphi((h_1^{-1})^{-1})(n_2) \varphi(h_1)(n_1^{-1})) \\
&= (h_1, n_1)(h_2 h_1^{-1}, \varphi(h_1)(n_2 n_1^{-1})) \\
&= (h_1 h_2 h_1^{-1}, \varphi((h_2 h_1^{-1})^{-1})(n_1)(\varphi(h_1)(n_2 n_1^{-1}))) \\
&= (h_1 h_2 h_1^{-1}, \varphi(h_1 h_2^{-1})(n_1)(\varphi(h_1)(n_2 n_1^{-1})))
\end{aligned}$$

Note that this can also be written as:

$$(h_1 h_2 h_1^{-1}, \varphi(h_1)(\varphi(h_2^{-1})(n_1) n_2 n_1^{-1}))$$

Attempts to reconcile differences

Note if $m : G \times G \rightarrow G$, is a group operation, and $\iota : G \rightarrow G$ is group inversion,

Is $m'(g, h) = m(h, g)$ is the opposite group, with same inversion? $m'(m'(g, h), k) = m'(m(h, g), k) = m(k, m(h, g)) = m(m(k, h), g) = m(m'(h, k), g) = m'(g, m'(h, k))$
 And, $m'(g, e) = m(e, g) = g = m(g, e) = m'(e, g)$, and $m'(g, \iota(g)) = m(\iota(g), g) = e = m(g, \iota(g)) = m'(\iota(g), g)$.

Let $A : G \times X \rightarrow X$ be a group action, i.e.

$$A(g, A(h, x)) = A(m(g, h), x) \text{ and}$$

$$A(e, x) = x.$$

Now let $A'(g, x) = A(\iota(g), x)$

Note

$$A(g, A'(g, x)) = A(g, A(\iota(g), x)) = A(m(g, \iota(g)), x) = A(e, x) = x.$$

And similarly,

$$A'(g, A(g, x)) = A(\iota(g), A(g, x)) = A(m(\iota(g), g), x) = A(e, x) = x.$$

Note:

$$\begin{aligned} A'(g, A'(h, x)) &= A(\iota(g), A(\iota(h), x)) \\ &= A(m(\iota(g), \iota(h)), x) \\ &= A(\iota(m(h, g)), x) \\ &= A'(m(h, g), x) \\ &= A'(m'(g, h), x). \end{aligned}$$

Clearly, $A'(e, x) = A(\iota(e), x) = A(e, x) = x$.

So A' is a group action with the opposite group.

Now note,

If we let $A(h, n) = \varphi(h)(n)$, then $A'(h, n) = A(\iota_H(h), n) = \varphi(\iota_H(h))(n) = \varphi(h^{-1})(n)$.

$$\begin{aligned} M_1((h_1, n_1), (h_2, n_2)) &= (m_H(h_1, h_2), m_N(n_1, \varphi(h_1)(n_2))) \\ &= (m_H(h_1, h_2), m_N(n_1, A(h_1, n_2))) \end{aligned}$$

$$\begin{aligned} M_2((h_1, n_1), (h_2, n_2)) &= (m_H(h_1, h_2), m_N(\varphi(h_2^{-1})(n_1), n_2)) \\ &= (m_H(h_1, h_2), m_N(A'(h_2, n_1), n_2)) \\ &= (m_H(h_1, h_2), m'_N(n_2, A'(h_2, n_1))) \\ &= (m'_H(h_2, h_1), m'_N(n_2, A'(h_2, n_1))) \end{aligned}$$

Note that, the opposite of M_2 without primes is same as M_1 . In other words, the first operation on opposite order, on the opposite operation on H and N respectively, with the “opposite” action, gives the second operation. Hence the two constructions are parallel.

Also note:

$$\begin{aligned} \iota_1((h, n)) &= (\iota_H(h), \varphi(\iota_H(h))(\iota_N(n))) \\ &= (\iota_H(h), A(\iota_H(h), \iota_N(n))) \\ \iota_2((h, n)) &= (\iota_H(h), \varphi(h)(\iota_N(n))) \\ &= (\iota_H(h), A(h, \iota_N(n))) \\ &= (\iota_H(h), A'(\iota_H(h), \iota_N(n))) \end{aligned}$$

Group Action on a Group - Furthermore when a group action is on a group, and preserves multiplication: i.e. $A : H \times N \rightarrow N$, is such that $A(h, -) : N \rightarrow N$ is a group automorphism for each $h \in H$, then we have the properties:

$$A(h, m_N(n_1, n_2)) = m_N(A(h, n_1), A(h, n_2))$$

and

$$A(h, \iota_N(n)) = \iota_N(A(h, n))$$

and

$$A(h, e_N) = e_N.$$

Remark Group inversion is an isomorphism between a group and its opposite, since we have:

$$\iota(m'(h, g)) = \iota(m(g, h)) = m(\iota(h), \iota(g))$$

and similarly,

$$\iota(m(g, h)) = m(\iota(h), \iota(g)) = m'(\iota(g), \iota(h))$$

8. SERRE-TANIYAMA GROUP

8.1. NOTATION, BACKGROUND

If G is an algebraic group over a field K and K' is a commutative K -algebra, $G(K')$ is the group of K' -points of G .

When K' is a field, $G_{/K'}$ is the K' -algebraic group $G \times_K K'$ obtained from G by extending the ground field from K to K' .

As an example,

$$\mathrm{GL}_V(K') = \mathrm{Aut}_{K'}(V \otimes_K K')$$

8.2. KRULL TOPOLOGY ON GALOIS GROUPS OF INFINITE EXTENSIONS

$\mathrm{Gal}(L/K) = \varprojlim_M \mathrm{Gal}(M/K)$ where the projective limit is taken over finite Galois extensions M over K , that are included in L . If $M_1 \geq M_2 \geq K$, are finite Galois extensions, then the morphism used to define the projective limit is restriction

$$r_{M_1, M_2}(\phi) = \phi|_{M_2}$$

where $\phi \in \mathrm{Gal}(M_1/K)$, and hence $\phi|_{M_2} \in \mathrm{Gal}(M_2/K)$. Since M_2 is a Galois extension of K , $\phi(M_2) = M_2$.

$G = \mathrm{Gal}(K_s/K)$ the Galois group of the separable algebraic closure of K with Krull topology is Hausdorff, compact and totally disconnected, i.e. a profinite group.

Note that $\mathrm{Gal}(L/M)$ are subsets of $\mathrm{Gal}(L/K)$ when $L \geq M \geq K$.

Since the topology on the projective limit is inherited from the product topology, projective limit being a subset of product of the groups, the neighborhoods of the topology on the projective limit of finite groups equipped with discrete topology are given by:

Neighborhoods of $\varprojlim_M \mathrm{Gal}(M/K)$ are intersections of neighborhoods of $\prod_M \mathrm{Gal}(M/K)$ with $\varprojlim_M \mathrm{Gal}(M/K)$. A neighborhood basis for $\prod_M \mathrm{Gal}(M/K)$ is given by $\prod_{M \neq M_0} \mathrm{Gal}(M/K) \times \{g\}$ where $g \in \mathrm{Gal}(M_0/K)$, where singletons are open since $\mathrm{Gal}(M_0/K)$ has discrete topology. But taking the intersection of this generic neighborhood with $\varprojlim_M \mathrm{Gal}(M/K)$, we get a set whose projection on M_0 component consists of the

singleton $\{g\}$, hence whose projections on all components $M \leq M_0$ consist of the projection of the singleton on those components. Since there are only finitely many extensions M with $K \leq M \leq M_0$, here M_0 and M being finite Galois over K , nothing is changed if we replace the neighborhood with

$$\prod_{M \not\leq M_0} \text{Gal}(M/K) \times \prod_{M \leq M_0} \{r_{M_0, M}(g)\}$$

which is also a neighborhood in $\prod_M \text{Gal}(M/K)$. Now we can see that the intersection of this with $\varprojlim_M \text{Gal}(M/K)$ is a translate of $\text{Gal}(L/M)$, if nonempty, by taking any element and translating the neighborhood by the inverse of that element.

Now also note $[\text{Gal}(L/K) : \text{Gal}(L/M)] = [M : K]$, since

$$\text{Gal}(L/K)/\text{Gal}(L/M) \cong \text{Gal}(M/K),$$

and M is Galois. Hence $\text{Gal}(L/M)$ is an open normal subgroup of $\text{Gal}(L/K)$, of finite index. Furthermore by Galois correspondence all open normal subgroups of finite index are of this form. Also note that since the cosets of $\text{Gal}(L/M)$ are open, their union excluding $\text{Gal}(L/M)$ is also open, hence $\text{Gal}(L/M)$ is closed. This is true for any open subgroup of any topological group.

8.3. ENLARGING GROUP

This theorem is stated in [84] II-3.

Theorem 20 *Let the following be assumed.*

- $k : \text{field}$
- $A : \text{commutative algebraic group over } k$
- $0 \rightarrow Y_1 \rightarrow Y_2 \rightarrow Y_3 \rightarrow 0$ exact sequence of commutative groups, with $Y_3 : \text{finite}$.
- $\varepsilon : Y_1 \rightarrow A(k)$ homomorphism of Y_1 into the group of k -rational points of A (it is assumed that the homomorphism utilizes addition of A)

Then there exists an algebraic group B with a morphism of algebraic groups $A \rightarrow B$ and homomorphism $Y_2 \rightarrow B(k)$ such that the diagram $Y_1 \longrightarrow A(k)$ is commutative. Hence

$$\begin{array}{ccc} Y_1 & \longrightarrow & A(k) \\ \downarrow & & \downarrow \\ Y_2 & \longrightarrow & B(k) \end{array}$$

we have the commutative diagram of exact sequences

$$\begin{array}{ccccccc} 0 & \longrightarrow & Y_1 & \longrightarrow & Y_2 & \longrightarrow & Y_3 \longrightarrow 0 \\ & & \downarrow \varepsilon & & \downarrow & & \downarrow \\ 0 & \longrightarrow & A(k) & \longrightarrow & B(k) & \longrightarrow & Y_3 \longrightarrow 0 \end{array}$$

B is universal with respect to the above, i.e. if B' satisfies same commutative diagram, then there exists a unique algebraic morphism $f : B \rightarrow B'$ i.e. we have the commutative diagram

$$\begin{array}{ccc} Y_1 & \longrightarrow & Y_2 \\ \downarrow & & \downarrow \\ A(k) & \longrightarrow & B(k) \\ & \searrow & \searrow \\ & & B'(k) \end{array}$$

Proof.

Identify Y_1 with its image in Y_2 . Let $p : Y_2 \rightarrow Y_3$ be the surjective projection map. Note that $\ker p = Y_1$, by exactness.

Choose a section $s : Y_3 \rightarrow Y_2$. (So that $p \circ s = \text{id.}$) Let

$$c(y_1, y_2) = s(y_1) + s(y_2) - s(y_1 + y_2)$$

Note that $c(y_1, y_2) \in Y_1$ by exactness, since $p(c(y_1, y_2)) = p(s(y_1) + s(y_2) - s(y_1 + y_2)) = 0$.

Let $B = \sqcup_{y \in Y_3} A_y$ where A_y is a copy of A . Since Y_3 is finite, affine cover of A gives an affine cover of B , making B a variety.

Define group law on B via

$$\pi_{y_1, y_2} : A_{y_1} \times A_{y_2} \rightarrow A_{y_1 + y_2}$$

for $y_1, y_2 \in Y_3$ by $\pi_{y_1, y_2}(a_1, a_2) = a_1 + a_2 + \varepsilon(c(y_1, y_2))$

In order to aid the notation, note that $B = A \times Y_3$ as sets.

Group law on B is defined by the following:

$$(a_1, y_1)(a_2, y_2) = (a_1 + a_2 + \varepsilon(c(y_1, y_2)), y_1 + y_2)$$

Note that we have chosen multiplicative notation for the group operation on B . However, it will turn out that B is also an abelian group.

Define $\iota : A \rightarrow B$ by $A \rightarrow A_0$ followed by translation $-\varepsilon(c(0,0))$ i.e. $a \mapsto (a - \varepsilon(c(0,0)), 0)$

Lemma 87 $\iota : A \rightarrow B$ defined by $a \mapsto (a - \varepsilon(c(0,0)), 0)$ is a group homomorphism.

Note that $a_1 - \varepsilon(c(0,0)) + a_2 - \varepsilon(c(0,0)) + \varepsilon(c(0,0)) = a_1 + a_2 - \varepsilon(c(0,0))$. This proves that $\iota(a_1)\iota(a_2) = \iota(a_1 + a_2)$.

Every element of Y_2 can be written in the form $s(y) + z$ for $y \in Y_3$ and $z \in Y_1$. Let $j : Y_2 \rightarrow B(k)$ be defined by mapping $u = s(y) + z$ (with y being the projection of u on Y_3) onto image of z in A_y .

In other words, $j : Y_2 \rightarrow B(k)$ maps $u = s(y) + (u - s(y)) = (u - s(y), y) \in Y_2$ to $(\varepsilon(u - s(y)), y)$. For this to be defined, we must have $u - s(y) \in Y_1$, but $p(u - s(y)) = p(u) - p(s(y)) = p(u) - y = 0$.

i.e.

$$j(y) = (\varepsilon(y - s(p(y))), p(y))$$

We will see later that this is a group homomorphism.

Let's check that it indeed fits into a commutative diagram.

Lemma 88 $\iota : A \rightarrow B$ defined by $\iota(a) = (a - \varepsilon(c(0,0)), 0)$ and $j : Y_2 \rightarrow B$ defined by $j(y) = (\varepsilon(y - s(p(y))), p(y))$ fit into a commutative diagram:

$$\begin{array}{ccc} Y_1 & \longrightarrow & Y_2 \\ \downarrow \varepsilon & & \downarrow j \\ A & \xrightarrow{\iota} & B \end{array}$$

Now checking commutativity of square on left:

The composition $Y_1 \xrightarrow{\varepsilon} A(k) \rightarrow B(k)$ is given by

$$y \mapsto (\varepsilon(y) - \varepsilon(c(0,0)), 0) \in B(k) = A(k) \times Y_3$$

The composition

$Y_1 \rightarrow Y_2 \rightarrow B(k)$ is given by $y \mapsto (\varepsilon(y - s(0)), 0)$ since $y \in Y_1$ implies that $p(y) = 0$, from the sequence.

Now from definition of c , we have $s(0) + s(0) - s(0 + 0) = s(0) = c(0, 0)$.

Therefore the composition $Y_1 \xrightarrow{\varepsilon} A(k) \rightarrow B(k)$ and the composition $Y_1 \rightarrow Y_2 \rightarrow B(k)$ coincide.

Lemma 89 *The operation on $B = A \times Y_3$ defined by*

$$(a_1, y_1)(a_2, y_2) = (a_1 + a_2 + \varepsilon(c(y_1, y_2)), y_1 + y_2)$$

makes B an abelian group.

Let's checking that group law is indeed a group law.

Associativity

$$\begin{aligned} ((a_1, y_1)(a_2, y_2))(a_3, y_3) &= (a_1 + a_2 + \varepsilon(c(y_1, y_2)), y_1 + y_2)(a_3, y_3) \\ &= (a_1 + a_2 + \varepsilon(c(y_1, y_2)) + a_3 + \varepsilon(c(y_1 + y_2, y_3)), y_1 + y_2 + y_3) \end{aligned}$$

on the other hand

$$\begin{aligned} (a_1, y_1)((a_2, y_2)(a_3, y_3)) &= (a_1, y_1)(a_2 + a_3 + \varepsilon(c(y_2, y_3)), y_2 + y_3) \\ &= (a_1 + a_2 + a_3 + \varepsilon(c(y_2, y_3)) + \varepsilon(c(y_1, y_2 + y_3)), y_1 + y_2 + y_3) \end{aligned}$$

We need to verify that

$$\varepsilon(c(y_1, y_2)) + \varepsilon(c(y_1 + y_2, y_3)) = \varepsilon(c(y_2, y_3)) + \varepsilon(c(y_1, y_2 + y_3))$$

This is a matter of simple computation, from definition of c

$$\begin{aligned}
 c(y_1, y_2) + c(y_1 + y_2, y_3) &= s(y_1) + s(y_2) - s(y_1 + y_2) \\
 &\quad + s(y_1 + y_2) + s(y_3) - s(y_1 + y_2 + y_3) \\
 &= s(y_1) + s(y_2) + s(y_3) - s(y_1 + y_2 + y_3)
 \end{aligned}$$

$$\begin{aligned}
 c(y_2, y_3) + c(y_1, y_2 + y_3) &= s(y_2) + s(y_3) - s(y_2 + y_3) \\
 &\quad + s(y_1) + s(y_2 + y_3) - s(y_1 + y_2 + y_3) \\
 &= s(y_2) + s(y_3) + s(y_1) - s(y_1 + y_2 + y_3)
 \end{aligned}$$

Commutativity Operation on $B(k)$ is commutative:

$$(a, y)(b, z) = (a + b + \varepsilon(c(y, z)), y + z)$$

and

$$(b, z)(a, y) = (b + a + \varepsilon(c(z, y)), z + y)$$

But operation on $A(k)$ and Y_3 is commutative, and

$$c(y, z) = s(y) + s(z) - s(y + z) = s(z) + s(y) - s(z + y) = c(z, y)$$

since operation on Y_2 is commutative.

Identity Identity of $B(k)$ is $(-\varepsilon(s(0)), 0) \in A \times Y_3$.

Note that $(a, y)(-\varepsilon(s(0)), 0) = (a - \varepsilon(s(0)) + \varepsilon(c(y, 0)), y)$

But $c(y, 0) = s(y) + s(0) - s(y + 0) = s(0)$, so $(a, y)(-\varepsilon(s(0)), 0) = (a, y)$.

Inverse of $(a, y) \in B(k)$ is $(-a - \varepsilon(c(y, -y)) - \varepsilon(c(0, 0)), -y)$. This is demonstrated below:

Note $c(y, -y) = s(y) + s(-y) - s(0)$, so that $c(y, -y) + c(0, 0) = s(y) + s(-y) - s(0) + s(0) + s(0) - s(0) = s(y) + s(-y)$

Note

$$\begin{aligned}
 & (a, y)(-a - \varepsilon(c(y, -y)) - \varepsilon(c(0, 0)), -y) \\
 &= (a - a - \varepsilon(c(y, -y)) - \varepsilon(c(0, 0)) + \varepsilon(c(y, -y)), y - y) \\
 &= (-\varepsilon(c(0, 0)), 0) \\
 &= (-\varepsilon(s(0)), 0)
 \end{aligned}$$

This proves that the inverse of (a, y) is indeed $(-a - \varepsilon(c(y, -y)) + c(0, 0)), -y)$.

Lemma 90 $j : Y_2 \rightarrow B(k)$ defined by $j(y) = (\varepsilon(y - s(p(y))), p(y))$ is a homomorphism.

$$\begin{aligned}
 & (\varepsilon(y_1 - s(p(y_1))), p(y_1))(\varepsilon(y_2 - s(p(y_2))), p(y_2)) = \\
 & (\varepsilon(y_1 - s(p(y_1))) + \varepsilon(y_2 - s(p(y_2))) + \varepsilon(c(p(y_1), p(y_2))), p(y_1) + p(y_2)) = \\
 & (\varepsilon(y_1 - s(p(y_1)) + y_2 - s(p(y_2)) + c(p(y_1), p(y_2))), p(y_1 + y_2)) = \\
 & (\varepsilon(y_1 - s(p(y_1)) + y_2 - s(p(y_2)) + s(p(y_1)) + s(p(y_2)) - s(p(y_1 + y_2))), p(y_1 + y_2)) = \\
 & (\varepsilon(y_1 + y_2 - s(p(y_1 + y_2))), p(y_1 + y_2)) =
 \end{aligned}$$

This establishes that $j(y_1)j(y_2) = j(y_1 + y_2)$.

Since $j(y)j(-y) = j(0) = (\varepsilon(0 - s(p(0))), p(0)) = (\varepsilon(-s(0)), 0)$ which is the identity of B , j maps inverses to inverses.

Lemma 91 *B is universal among groups B' that fit into a commutative diagram:*

$$\begin{array}{ccc} Y_1 & \longrightarrow & Y_2 \\ \downarrow & & \downarrow \\ A & \longrightarrow & B' \end{array}$$

Proof of universality:

Let $(a, y) \in B(k)$.

Note that under the operation in $B(k)$, we have

$$(a, y) = (a - \varepsilon(c(0, 0)), 0)(0, y)$$

which can also be expressed in the form

$$(a, y) = \iota(a)j(s(y))$$

since $c(0, 0) = c(0, y) = s(0)$

Now $(a - \varepsilon(c(0, 0)), 0)$ is in the image of the map $A(k) \rightarrow B(k)$, in particular a maps to this element. And $(0, y)$ is in the image of the map $Y_2 \rightarrow B(k)$. In particular,

$s(y)$ maps to $(0, y)$ under this map, since

$$\varepsilon(s(y) - s(p(s(y)))) = \varepsilon(s(y) - s(y)) = \varepsilon(0) = 0$$

Now if $f_1 : A(k) \rightarrow B'(k)$ and $f_2 : Y_2 \rightarrow B'(k)$ are given,

we define $f : B(k) \rightarrow B'(k)$ by

$$f(a, y) = f_1(a)f_2(s(y))$$

In order to motivate this definition, note the following:

If $f : B(k) \rightarrow B'(k)$ satisfies commutative diagram, we should have

$$f \circ \iota = f_1 \text{ and } f \circ j = f_2.$$

If f is to be a homomorphism, then

$$f(a, y) = f(\iota(a)j(s(y))) = f(\iota(a))f(j(s(y))) = f_1(a)f_2(s(y)).$$

This establishes uniqueness of f .

Proving that f is a homomorphism:

Note that

$$\begin{aligned} f((a_1, y_1)(a_2, y_2)) &= f((a_1 + a_2 + \varepsilon(c(y_1, y_2)), y_1 + y_2)) \\ &= f_1(a_1 + a_2 + \varepsilon(c(y_1, y_2)))f_2(s(y_1 + y_2)) \\ &= f_1(a_1 + a_2)f_1(\varepsilon(c(y_1, y_2)))f_2(s(y_1 + y_2)) \end{aligned}$$

But note that by commutativity we have $f_1\varepsilon = f_2$ (where inclusion of Y_1 in Y_2 on the right side of the equality is suppressed) so we have

$$\begin{aligned} &= f_1(a_1 + a_2)f_2(c(y_1, y_2))f_2(s(y_1 + y_2)) \\ &= f_1(a_1 + a_2)f_2(s(y_1) + s(y_2) - s(y_1 + y_2))f_2(s(y_1 + y_2)) \\ &= f_1(a_1 + a_2)f_2(s(y_1) + s(y_2) - s(y_1 + y_2) + s(y_1 + y_2)) \\ &= f_1(a_1 + a_2)f_2(s(y_1) + s(y_2)) \end{aligned}$$

and,

$$\begin{aligned}
f((a_1, y_1))f((a_2, y_2)) &= f_1(a_1)f_2(s(y_1))f_1(a_2)f_2(s(y_2)) \\
&= f_1(a_1 + a_2)f_2(s(y_1) + s(y_2))
\end{aligned}$$

So we have proved that

$$f((a_1, y_1)(a_2, y_2)) = f((a_1, y_1))f((a_2, y_2)).$$

This concludes the proof of universality.

Remark

In the language of group cohomology, the section $s : Y_3 \rightarrow Y_2$ is a 1-cochain, i.e. an element of $C^1(Y_3, Y_2)$. The map $c : Y_3 \times Y_3 \rightarrow Y_2$ whose image is actually in Y_1 by exactness of the sequence, is given by

$$c(x, y) = s(x) + s(y) - s(x + y) = d_1(s)(x, y)$$

Therefore, c is a 1-coboundary, i.e. an element of $B^1(Y_3, Y_2)$. Hence it is also a 2-cocycle, i.e. an element of $Z^2(Y_3, Y_2)$ (and also $Z^2(Y_3, Y_1)$, since image of c lies in image of Y_1 in Y_2 .)

This means that

$$d_2(c)(x, y, z) = xc(y, z) - c(x + y, z) + c(x, y + z) - c(x, y) = 0$$

Here we are assuming that the group action is trivial (since the groups are abelian), so that this is equal to $c(y, z) - c(x + y, z) + c(x, y + z) - c(x, y)$. This can be verified easily from definition of c .

$$c(y, z) = s(y) + s(z) - s(y + z)$$

$$-c(x + y, z) = -s(x + y) - s(z) + s(x + y + z)$$

$$c(x, y + z) = s(x) + s(y + z) - s(x + y + z)$$

$$-c(x, y) = -s(x) - s(y) + s(x + y)$$

If the section s were a homomorphism, then this would mean that s is a 1-cocycle. It also means that the sequence $0 \rightarrow Y_1 \rightarrow Y_2 \rightarrow Y_3 \rightarrow 0$ is split-exact.

2-cocycles $Z^2(G, A)$ modulo 1-coboundaries (i.e. cohomology classes in $H^2(G, A)$) determine different extension classes of G by A .

Lemma 92 *If $\varepsilon : Y_1 \rightarrow A(k)$ is injective, then so is $j : Y_2 \rightarrow B$.*

This follows from diagram-chasing. If $j(y) = 0$, then $p(y) = \tilde{p}j(y) = 0$, from commutativity of the diagram, where $\tilde{p} : B(k) \rightarrow Y_3$ is the projection in the lower exact sequence, defined by $\tilde{p}(a, y') = y'$.

By exactness of the sequence $0 \rightarrow Y_1 \rightarrow Y_2 \rightarrow Y_3 \rightarrow 0$, since $p(y) = 0$, we have that $y \in Y_1$. Rather y is the image of some unique element in Y_1 , but we have identified these at the beginning.

Now by commutativity of the diagram, $\iota\varepsilon(y) = j(y) = 0$. Since ι is injective, this means that $y \in \ker \varepsilon$, but by assumption ε is injective, so $y = 0$, establishing injectivity of j .

Lemma 93 *If $\varepsilon : Y_1 \rightarrow A_k$ is surjective, then so is j .*

Let (a, y) be a general element of B .

We have that $(a, y) = \iota(a)j(s(y))$. But surjectivity of ε means that there is some $\tilde{a}$ such that $\varepsilon(\tilde{a}) = a$, so that we have

$$(a, y) = \iota(\varepsilon(\tilde{a}))j(s(y))$$

and commutativity of diagram means that $\iota\varepsilon = j$, so that

$$(a, y) = j(\tilde{a})j(s(y)) = j(\tilde{a}s(y)),$$

which establishes that j is surjective.

Lemma 94 Y_2 is isomorphic to $B(k)$ formed by taking $A(k) = Y_1$, and $\varepsilon = \text{id}$.

This is a consequence of the previous two lemmas.

Lemma 95 If the section $s : Y_3 \rightarrow Y_2$ can be chosen as a group homomorphism, then $Y_2 = Y_1 \times Y_3$.

This is a consequence of the previous lemma.

Theorem 21 If $\varepsilon_1 : Y_1 \rightarrow A$ yields the extension $A \rightarrow B \rightarrow Y_3$ from the exact sequence $0 \rightarrow Y_1 \rightarrow Y_2 \rightarrow Y_3 \rightarrow 0$, and $\varepsilon_2 : A \rightarrow A'$ yields the extension $A' \rightarrow B' \rightarrow Y_3$, then $\varepsilon_3 = \varepsilon_2 \circ \varepsilon_1$ yields the same extension.

Proof.

We are going to assume that we have the commutative diagrams:

$$\begin{array}{ccccccc} 0 & \longrightarrow & Y_1 & \longrightarrow & Y_2 & \xrightarrow{p} & Y_3 \longrightarrow 0 \\ & & \downarrow \varepsilon_1 & & \downarrow j_1 & & \downarrow \\ 0 & \longrightarrow & A & \xrightarrow{\iota_1} & B & \xrightarrow{p_1} & Y_3 \longrightarrow 0 \\ & & \downarrow \varepsilon_2 & & \downarrow j_2 & & \downarrow \\ 0 & \longrightarrow & A' & \xrightarrow{\iota_2} & B' & \xrightarrow{p_2} & Y_3 \longrightarrow 0 \end{array}$$

and

$$\begin{array}{ccccccc} 0 & \longrightarrow & Y_1 & \longrightarrow & Y_2 & \xrightarrow{p} & Y_3 \longrightarrow 0 \\ & & \downarrow \varepsilon_3 & & \downarrow j_3 & & \downarrow \\ 0 & \longrightarrow & A' & \xrightarrow{\iota_3} & B'' & \xrightarrow{p_3} & Y_3 \longrightarrow 0 \end{array}$$

Now from universality, we know that there is a group homomorphism $f : B'' \rightarrow B'$ such that

$$f \circ j_3 = j_1 \circ j_2, \text{ and } f \circ \iota_3 = \iota_2.$$

But we will see shortly that in fact, B' and B'' are isomorphic.

We are going to assume that $s_1 : Y_3 \rightarrow Y_2$ is a section of $p : Y_2 \rightarrow Y_3$. And that determines the structures.

For the splitting of the second sequence we will choose $s_2 : Y_3 \rightarrow B$ defined by $s_2(y) = (0, y)$. So that we have

$$\tilde{c}_2(y, z) = s_2(y)s_2(z)s_2(y+z)^{-1}$$

Evaluating this gives

$$\begin{aligned} \tilde{c}_2(y, z) &= s_2(y)s_2(z)s_2(y+z)^{-1} \\ &= (0, y)(0, z)(0, y+z)^{-1} \\ &= (\varepsilon_1 c_1(y, z), y+z)(-\varepsilon_1(c_1(y+z, -y-z) + c_1(0, 0)), -y-z) \\ &= (\varepsilon_1 c_1(y, z) - \varepsilon_1(c_1(y+z, -y-z) - c_1(0, 0)) + \varepsilon_1(c_1(y+z, -y-z)), 0) \\ &= (\varepsilon_1(c_1(y, z)) - \varepsilon_1(c_1(0, 0)), 0) \\ &= \iota_1(\varepsilon_1(c_1(y, z))) \end{aligned}$$

Now define $c_2(y, z) = \varepsilon_1(c_1(y, z))$.

So that

$$\varepsilon_2(c_2(y, z)) = \varepsilon_2(\varepsilon_1(c_1(y, z))) = \varepsilon_3(c_1(y, z))$$

This establishes that B' and B'' are isomorphic as groups. Note that $B' = A' \times Y_3$ and $B'' = A' \times Y_3$ as a set. Since the factor $\varepsilon_2 c_2$ and $\varepsilon_3 c_1$ determines the group operation on B' and B'' respectively, the above equality establishes that B' , and B'' are isomorphic as groups.

$\iota_2 = \iota_3$. (Of course this is not entirely true, since B' and B'' appear as different groups, but there is a canonical isomorphism between them described above.)

Note $\iota_2(a) = (a - \varepsilon_2(c_2(0, 0)), 0) = (a - \varepsilon_2(\varepsilon_1(c_1(0, 0))), 0) = (a - \varepsilon_3(c_1(0, 0)), 0) = \iota_3(a)$.

Now for the remainder of the proof, it suffices to prove that if $j_1 : Y_2 \rightarrow B$ and $j_2 : B \rightarrow B'$ denote the homomorphisms in the corresponding commutative diagrams, then $j_3 : Y_2 \rightarrow B'$ satisfies

$$j_3 = j_2 \circ j_1$$

Now

$$j_3(y) = (\varepsilon_3(y - s_1 p(y)), p(y))$$

Let's compute $j_2 \circ j_1$ in stages:

$$j_2(y) = (\varepsilon_2(y - s_2 p_1(y)), p_1(y))$$

But here there is some minor abuse of notation. Since $p_1(y - s_2 p_1(y)) = 0$, there exists $\tilde{a}_y \in A$ such that $\iota_1(\tilde{a}_y) = y - s_2 p_1(y)$. So by $\varepsilon_2(y - s_2 p_1(y))$ is meant $\varepsilon_2(\tilde{a}_y)$.

$$j_1(y) = (\varepsilon_1(y - s_1 p(y)), p(y))$$

So that

$$p_1(j_1(y)) = p(y)$$

Recall $s_2(y') = (0, y')$. (We will re-establish independence of extension from choice of section. This is already guaranteed by universality.)

Now computing the argument of $\varepsilon_2(\cdot)$ for evaluation of $j_2 \circ j_1(y)$ is carried out below:

$$\begin{aligned}
& j_1(y) - s_2 p_1(j_1(y)) \\
&= (\varepsilon_1(y - s_1 p(y)), p(y))(0, p(y))^{-1} \\
&= (\varepsilon_1(y - s_1 p(y)), p(y))(-\varepsilon_1(c_1(p(y), -p(y)) + c_1(0, 0)), -p(y)) \\
&= (\varepsilon_1(y - s_1 p(y)) - \varepsilon_1(c_1(p(y), -p(y))) - \varepsilon_1(c_1(0, 0)) + \varepsilon_1(c_1(p(y), -p(y))), 0) \\
&= (\varepsilon_1(y - s_1 p(y)) - \varepsilon_1(c_1(0, 0)), 0) \\
&= \iota_1(\varepsilon_1(y - s_1 p(y)))
\end{aligned}$$

So then we have

$$\begin{aligned}
j_2 \circ j_1(y) &= (\varepsilon_2(j_1(y) - s_2 p_1(j_1(y))), p_1(j_1(y))) \\
&= (\varepsilon_2(\iota_1(\varepsilon_1(y - s_1 p(y)))), p(y)) \\
&= (\varepsilon_2(\varepsilon_1(y - s_1 p(y))), p(y)) \\
&= (\varepsilon_3(y - s_1 p(y)), p(y)) \\
&= j_3(y)
\end{aligned}$$

This means that the two commutative diagrams at the beginning fit together into a single commutative diagram, with the map between B' and B'' being basically identity.

$$\begin{array}{ccccc}
& Y_1 & \xrightarrow{\quad} & Y_2 & \xrightarrow{p} & Y_3 \\
& \swarrow \varepsilon_1 & & \swarrow j_1 & & \swarrow \\
A & \xrightarrow{\quad} & B & \xrightarrow{p_1} & Y_3 & \\
& \searrow \varepsilon_2 & & \searrow j_2 & & \searrow \\
& & \varepsilon_3 & & j_3 & \\
& & A' & \xrightarrow{\iota_2 = \iota_3} & B' = B'' & \xrightarrow{p_2 = p_3} & Y_3
\end{array}$$

Remark 1 We can apply the theorem we just proved with extensions of k .

Remark 2 A character of B , which is a (continuous or algebraic) group homomorphism from B to the multiplicative group of $\bar{k}$ or to $\mathbf{C}$, determines characters of Y_2 and A , by composition with $j : Y_2 \rightarrow B$ and $\iota : A \rightarrow B$. Furthermore given a pair (ϕ, χ) of characters of A and Y_2 respectively, that agree on Y_1 , form a commutative square. i.e. if $\phi \circ \varepsilon = \chi$ with Y_1 in Y_2 identified with Y_1 , then by universality there is a group homomorphism from B to $\mathbf{C}$ i.e. a character of B . In other words, if $X(G)$ denotes the character group of G , and for a group homomorphism $f : G \rightarrow H$, $X(f) : X(H) \rightarrow X(G)$ is defined by $X(f)(\chi) = \chi \circ f$ then we have the commutative diagram:

$$\begin{array}{ccc}
X(B) & \xrightarrow{X(j)} & X(Y_2) \\
X(\iota) \downarrow & & \downarrow X(\iota_0) \\
X(A) & \xrightarrow{X(\varepsilon)} & X(Y_1)
\end{array}$$

corresponding to the commutative diagram

$$\begin{array}{ccc}
Y_1 & \xrightarrow{\iota_0} & Y_2 \\
\varepsilon \downarrow & & \downarrow j \\
A & \xrightarrow{\iota} & B
\end{array}$$

8.4. IDELÈS AND IDELÈS-CLASSES

- Σ_K : set of finite places of the number field K .
- Σ_K^∞ : set of equivalence classes of archimedean absolute values of K ,
- $\overline{\Sigma_K} = \Sigma_K \cup \Sigma_K^\infty$
- K_v : the completion of K with respect to v , for $v \in \overline{\Sigma_K}$

- For $v \in \Sigma_K^\infty$ we have $K_v = \mathbb{R}$ or $K_v = \mathbb{C}$,
- K_v is ultrametric if $v \in \Sigma_K$.
- U_v : group of units of (the ring of integers of) K_v for $v \in \Sigma_K$
- The idèle group

$$I = I_K = \{(a_v)_{v \in \overline{\Sigma_K}} \in \prod_{v \in \overline{\Sigma_K}} K_v^* \mid a_v \in U_v \text{ for almost all } v \in \overline{\Sigma_K}\}$$

This is also shown in the notation

$$\prod_{v \in \Sigma_K^\infty} K_v \times \prod_{v \in \Sigma_K}^* (K_v : U_v)$$

(for almost all means all but finitely many)

8.4.1. Topology of Idele Group.

(This is called a restricted product.) It is given a topology by decreeing that the subgroup (with the product topology)

$$\prod_{v \in \Sigma_K^\infty} K_v \times \prod_{v \in \Sigma_K} U_v$$

be open.

8.4.2. Embedding of K^* inside Ideles and Idele Class Group

We embed K^* into I by sending $a \in K^*$ onto the idèle (a_v) , where $a_v = a$ for all v . The topology induced on K^* is the discrete topology. The quotient group $C = I/K^*$ is called the idèle-class group of K .

8.4.3. Modulus of Support and Exact Sequence

Definition 166 Let S be a finite subset of Σ_K . Then by a modulus of support S we mean a family $m = (m_v)_{v \in S}$ where the m_v are integers ≥ 1 . We can think of a modulus as a function from Σ_K to $\mathbb{N}$, which assumes the value zero for all but finitely many values.

Definition 167 If $v \in \overline{\Sigma_K}$ and m is a modulus of support S , we let $U_{v,m}$ denote the connected component of K_v^* if $v \in \Sigma_K^\infty$ the subgroup of U_v consisting of those $u \in U_v$ for which $v(1-u) \geq m_v$ and U_v if $v \in \Sigma_K - S$.

In other words

$$U_{v,m} = \begin{cases} \text{the connected component of } K_v^* & \text{if } v \in \Sigma_K^\infty \\ 1 + \mathcal{M}_{K_v}^{m_v} = \{u \in U_v \mid v(1-u) \geq m_v\} & \text{if } v \in S \\ U_v & \text{if } v \in \Sigma_K - S. \end{cases}$$

where $\mathcal{M}_{K_v}$ is the maximal ideal of the ring of integers of K_v , i.e. those elements of the ring of integers of K_v that have valuation greater than or equal to 1.

$$U_m = \prod_v U_{v,m}$$

The group $U_m = \prod_v U_{v,m}$ is an open subgroup of I .

For m, n being nonnegative integers, we have:

Note that $(1 + \mathfrak{p}^m)(1 + \mathfrak{p}^n) = 1 + \mathfrak{p}^{\min\{m,n\}}$.

Explicitly

$$\begin{aligned} (1 + \mathfrak{p}^m)(1 + \mathfrak{p}^n) &= 1 + \mathfrak{p}^m + \mathfrak{p}^n + \mathfrak{p}^{m+n} \\ &= 1 + \mathfrak{p}^{\min\{m,n\}} (\mathfrak{p}^{m-\min\{m,n\}} + \mathfrak{p}^{n-\min\{m,n\}} + \mathfrak{p}^{m+n-\min\{m,n\}}) \\ &= 1 + \mathfrak{p}^{\min\{m,n\}} \end{aligned}$$

On the other hand, $1 + \mathfrak{p}^{m+1} \subset 1 + \mathfrak{p}^m$.

Now if R is a valuation ring, with unique maximal ideal $\mathfrak{m}$, then every element of $R - \mathfrak{m}$ is a unit. Hence $\mathcal{O}_{K_v} - \mathcal{M}_{K_v}$ consists of units U_v . But then $1 + \mathcal{M}_{K_v} \subset U_v$.

Hence $1 + \mathcal{M}_{K_v}^m$ is a multiplicative subgroup of U_v , for every nonnegative integer m and finite valuation v of K .

Let's also note that:

$$U_m \cap U_n = U_{\max\{m,n\}}$$

where $\max\{m, n\}$ has modulus of support $S_m \cup S_n$ and

$$\max\{m, n\}_v = \begin{cases} \max\{m_v, n_v\} & \text{if } v \in S_m \cap S_n \\ m_v & \text{if } v \in S_m - S_n \\ n_v & \text{if } v \in S_n - S_m. \end{cases}$$

And we also have

$$U_m \cdot U_n = U_{\min\{m, n\}}$$

where $\min\{m, n\}$ has modulus of support $S_m \cap S_n$ and $\min\{m, n\}_v = \min\{m_v, n_v\}$ for $v \in S_m \cap S_n$.

Definition 168 *If E is the group of units of K , let*

$$E_m = E \cap U_m.$$

The subgroup E_m is of finite index in E . Note that the different cosets will vary over multiplication modulo $\mathfrak{M}_{K_v}^{m_v}$ as v varies over the places in the modulus of support S of m . Since there are finitely many such classes, the index is finite.

(Conversely, by a theorem of Chevalley, every subgroup of finite index in E contains an E_m for a suitable modulus m .) Relevant sources are below: C. CHEVALLEY - Deux théorèmes d'arithmétique. J, Math. Soc. Japan, 3, 1951, p. 36-44. [19] J.-P. SERRE - Sur les groupes de congruence des variétés abéliennes. Izv. Akad. Nauk. S.S.S.R., 28, 1964, p. 3-20. no 3.5 [82]

Definition 169 • $I_m = I/U_m$

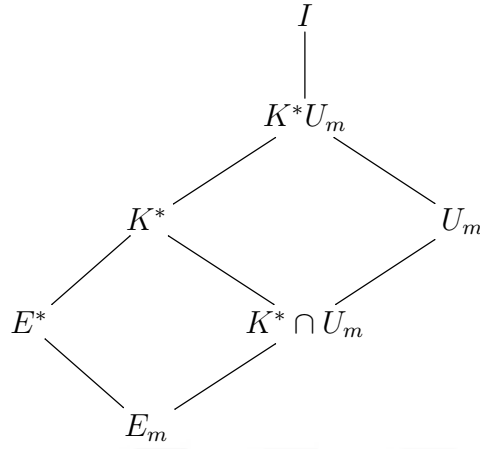
• $C_m = I/K^*U_m = C/(\text{Image of } U_m \text{ in } C).$

Remark, here $I \rightarrow C = I/K^*$ is the projection of ideles. $U_m \subset I$

One then has the exact sequence

$$1 \rightarrow K^*/E_m \rightarrow I_m \rightarrow C_m \rightarrow 1$$

Here note the lattice of subgroups



Note that the kernel of the map

$$I_m = I/U_m \rightarrow C_m = I/K^*U_m$$

is $K^*U_m/U_m = K^*/(K^* \cap U_m) = E^*/E_m$

Note that

$$C_m = I/K^*U_m = (I/K^*)/(K^*U_m/K^*) = C/(U_m/(K^* \cap U_m))$$

This should support the interpretation that we are dividing by the image of U_m in C

Furthermore, we claim that $K^* \cap U_m = E_m$.

Note that

$$K^* \cap U_m \subset K^* \cap \prod_{v \in \Sigma_K^\infty} K_v^{*o} \prod_{v \in \Sigma_K} U_v \subset \bigcap_{v \in \Sigma_K} K^* \cap U_v$$

But note that $K^* \cap U_v \subset \mathcal{O}_{K_{\mathfrak{p}}}$ where $\mathfrak{p}$ is the prime corresponding to finite valuation v , and $\mathcal{O}_K$ is the ring of integers of K , and $\mathcal{O}_{K_{\mathfrak{p}}}$ is the localization of $\mathcal{O}_K$ at the prime $\mathfrak{p}$.

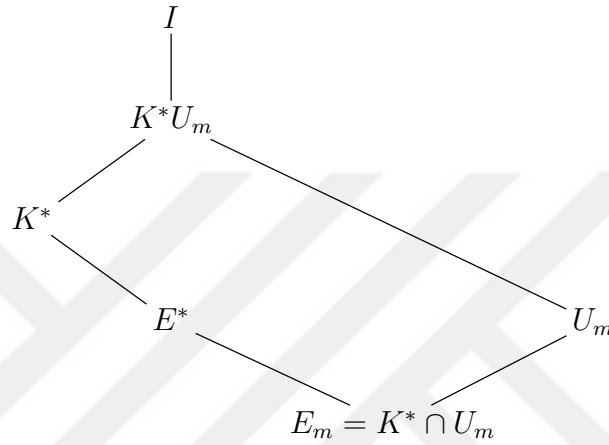
Now $\bigcap_{\mathfrak{p}} \mathcal{O}_{K_{\mathfrak{p}}} = \mathcal{O}_K$, since by definition $\mathcal{O}_K$ is integrally closed. For references to this statement, see Commutative Algebra by Zariski Samuel, and other sources.

Alternatively if $x \in K^* \cap U_m$, then $v(x) = 0$, for all finite valuations v of K , since $x \in K^* \cap U_v$. Hence the fractional ideal (x) , which can be factorized, K being a number field,

hence a Dedekind domain, in prime ideals of K , should have zero exponent in all the prime components, hence the ideal (x) is in fact the ring of integers of K .

This shows that $K^* \cap U_m \subset E$, hence $E_m = E \cap U_m = K^* \cap U_m$.

So the lattice of subgroups above should be corrected to :



8.5. RESTRICTION OF SCALARS

The excerpts are from Andre Weil's Adeles and Algebraic Groups. [97]

Restriction of the basic field.

Definition 170 • Let K/k be a separable algebraic extension of degree d ,

- Let V, W be varieties defined over K, k respectively (K/k not necessarily normal.)
- Let $p : W \rightarrow V$ be a map defined over K .
- Let $\Sigma = \{\sigma_1, \dots, \sigma_d\}$ be the set of all distinct isomorphisms of K into $\bar{k}$.
- We can then define $p^\sigma : W \rightarrow V^\sigma$ and $(p^{\sigma_1}, \dots, p^{\sigma_d}) : W \rightarrow V^{\sigma_1} \times \dots \times V^{\sigma_d}$.

If the latter map $(p^{\sigma_1}, \dots, p^{\sigma_d})$ gives an isomorphism, we call W (actually the pair $\{W, p\}$) the variety obtained from V by restriction of the field of definition from K to k and write $\{W, p\} = R_{K/k}(V)$

The primary example of restriction of scalars that we utilize is with the multiplicative group of the field, i.e. $R_{K/k}(G_{m/K})$ where $G_{m/K} = K^*$.

In the above definition, we take $W = K^* = V$, and $p = \text{id}$. However the difference is that V is a variety defined over K , and W is a variety defined over k .

For example if we take $K = \mathbb{Q}[x]/(x^2 - 2)$, then the restriction of scalars consists of the map:

$$p : K^* \rightarrow \bar{\mathbb{Q}} \times \bar{\mathbb{Q}}$$

defined by

$$p(a + bx) = (a + b\sqrt{2}, a - b\sqrt{2})$$

which is an isomorphism onto its image.

8.6. THE TORUS T

Given an algebraic group G over k , let G_{k_s} denote the restriction of G from k -algebras to k_s -algebras.

Definition 171 *An algebraic k -group G is a torus if G_{k_s} is a finite product of G'_m s. It is a split torus if it is a finite product of G'_m s. The condition for being a split-torus is equivalent to the Galois action being trivial.*

Remark As a result of the equivalent condition, the quotient of a split torus, its character group being a subgroup of the character group of the split torus, is also a split torus.

- $T = R_{K/Q}(G_{m/K})$ is the algebraic group over Q obtained from the multiplicative group G_m by restriction of scalars from K to Q
- If A is a commutative Q -algebra, the points of T with values in A form the multiplicative group $(K \otimes_Q A)^*$
- $T(Q) = K^*$
- If $[K : Q] = d$ then group T is a torus of dimension d i.e.

$$T_{/\bar{Q}} = T \times_Q \bar{Q}$$

obtained from T by extending the scalars from Q to $\bar{Q}$ is isomorphic to $(G_{m/\bar{Q}})^d$ i.e. $(\bar{Q}^*)^d$

- More precisely, if Γ is the set of embeddings of K in $\bar{Q}$, then
 - each $\sigma \in \Gamma$ extends to a homomorphism $K \otimes_Q \bar{Q} \rightarrow \bar{Q}$ (is this not an isomorphism)
 - hence defines a morphism $[\sigma] : T_{/\bar{Q}} \rightarrow G_{m/\bar{Q}}$
- The collection of all $[\sigma]$'s gives the isomorphism

$$T_{/\bar{Q}} \rightarrow G_{m/\bar{Q}} \times \dots \times G_{m/\bar{Q}}$$

- The $[\sigma]'$ form a basis of the character group $X(T) = \text{Hom}_{\bar{Q}}(T_{/\bar{Q}}, G_{m/\bar{Q}})$ of T .
- Galois group $\text{Gal}(\bar{Q}/Q)$ acts in a natural way on $X(T)$ by permuting $[\sigma]'$'s.

reference to [74], dictionary between tori and Galois modules.

8.6.1. Subgroups of Tori

- Let $E \leq K^* = T(Q)$ be a subgroup and $\bar{E}$ its Zariski closure in T .
-

$$\bar{E} \times \bar{E} = \overline{E \times E}$$

- $\bar{E}$ is an algebraic subgroup of T

Let

$$T_E = T/\bar{E}$$

- T_E is a torus over Q
- Its character group is

$$X_E = X(T_E) = \{\lambda \in X(T) \mid \lambda|_E = 1\}$$

i.e is a subgroup of the characters of T that take value 1 on E

- If $\lambda = \prod_{\sigma \in \Gamma} [\sigma]^{n_\sigma}$ denotes a character of T , then X_E is the subgroup of those $\lambda \in X$ for which $\prod \sigma(x)^{n_\sigma} = 1$ for all $x \in E$.

8.7. ALGEBRAIC TORI

G_m is the multiplicative group of the universal domain.

If O denotes a set of geometric objects, we shall denote by O_K the subset of O which is rational over a field K .

For a commutative algebraic group G ,

$$\hat{G} = \text{Hom}(G, G_m)$$

the set of all rational homomorphisms of G in G_m , or rational characters of G forms an abelian group.

$$\hat{G}_m \cong \mathbf{Z}, \text{ and } \widehat{(G_m)^d} = \mathbf{Z}^d.$$

For a module M ,

$$\hat{M} = \text{Hom}(M, G_m)$$

forms a group under multiplication.

Here Hom means homomorphisms of abelian groups and $\mathbf{Z}$ -modules, where G_m is a $\mathbf{Z}$ module by $nx = x^n$.

If $M = \mathbf{Z}$, identify $\hat{\mathbf{Z}}$ with G_m . One has $\hat{\mathbf{Z}}^d = (G_m)^d$.

Every element of $x \in G$ represents an element $\varphi_x \in \hat{G} = \text{Hom}(\hat{G}, G_m)$ by setting

$$\varphi_x(\xi) = \xi(x) \quad \xi \in \hat{G}$$

For $A \subset G$, and $B \subset \hat{G}$ annihilators are defined by

$$A^0 = \{\xi \in \hat{G}, \xi(x) = 1 \text{ for every } x \in A\}$$

$$B^0 = \{x \in G, \xi(x) = 1 \text{ for every } \xi \in B\}$$

Let G' be another commutative algebraic group, and $\alpha : G \rightarrow G'$ a homomorphism. Then $\hat{\alpha} : \hat{G}' \rightarrow \hat{G}$ is defined by

$$\hat{\alpha}(\xi') = \xi' \circ \alpha, \quad \xi' \in \hat{G}'$$

$\alpha \mapsto \hat{\alpha}$ is a homomorphism $\text{Hom}(G, G') \rightarrow \text{Hom}(\hat{G}', \hat{G})$.

Lemma 96 *If α (resp. $\hat{\alpha}$) is surjective, $\hat{\alpha}$ (resp. α) is injective.*

Proof of lemma

If α is surjective, then for every $g' \in G'$ there exists $g \in G$ such that $g' = \alpha(g)$. But then for any $\xi' \in \hat{G}'$, we have $\xi'(g') = \xi' \circ \alpha(g) = \hat{\alpha}(\xi')(g)$. If $\hat{\alpha}(\xi') = 1$, then $\xi'(g') = 1$. i.e. $\xi' = 1$. So $\hat{\alpha}$ is injective.

If $\hat{\alpha}$ is surjective, then for any $\xi \in \hat{G}$ there exists $\xi' \in \hat{G}'$ such that $\hat{\alpha}(\xi') = \xi$. If $\alpha(g) = 1$, then $\xi(g) = \hat{\alpha}(\xi')(g) = \xi' \circ \alpha(g) = 1$, so that $\xi = 1$. Hence α is injective.

Lemma 97 *For homomorphisms $G \xrightarrow{\alpha} G' \xrightarrow{\beta} G''$ one has $\widehat{\beta \circ \alpha} = \hat{\alpha} \circ \hat{\beta}$.*

$$\begin{aligned} \widehat{\beta \circ \alpha}(\xi'') &= \xi'' \circ \beta \circ \alpha \\ &= \hat{\beta}(\xi'') \circ \alpha \\ &= \hat{\alpha}(\hat{\beta}(\xi'')) \end{aligned}$$

Definition 172 *A torus is an algebraic group G isomorphic to $(G_m)^d$. If $f : G \rightarrow (G_m)^d$ is this isomorphism, then $\hat{f} : \mathbf{Z}^d \rightarrow \hat{G}$, is an isomorphism.*

Proposition 14 *Let T, T' be tori. Then*

- (1) $x \mapsto \varphi_x$ gives $T \cong \hat{\hat{T}}$,
- (2) $A \rightarrow A^0, B \rightarrow B^0$ define reciprocal bijections between the set of closed subgroups A of T and the set of submodules B of $\hat{T}$ such that $\hat{T}/B$ is p -torsion free, p being the characteristic exponent of the universal domain.
- (3) $\widehat{T/A} \cong A^0, \hat{A} \cong \hat{T}/A^0$ canonically.
- (4) $\alpha \mapsto \hat{\alpha}$ defined by $\hat{\alpha}(\xi') = \xi' \circ \alpha$ gives

$$\text{Hom}(T, T') \cong \text{Hom}(\hat{T}', \hat{T})$$

(5) α is an isomorphism if and only if $\hat{\alpha}$ is an isomorphism.

Proof of (1)

Short argument is as follows: for $T \cong (G_m)^d$, $\hat{G} = \text{Hom}((G_m)^d, G_m) = \text{Hom}(G_m, G_m)^d = \mathbb{Z}^d$, and $\hat{\hat{G}} = \text{Hom}(\mathbb{Z}^d, G_m) = (\text{Hom}(\mathbb{Z}, G_m))^d = G_m^d$.

The map $x \mapsto \varphi_x$ where $\varphi_x(\xi) = \xi(x)$, is clearly injective.

On the other hand, $\varphi_{xy}(\xi) = \xi(xy) = \xi(x)\xi(y) = \varphi_x(\xi)\varphi_y(\xi)$. So the map is an injective homomorphism of T into $\hat{\hat{T}}$.

Suppose $f \in \hat{\hat{G}}$, where $G = G_m^d$.

$$x_i = f(\pi_i)$$

where $\pi_i : G_m^d \rightarrow G_m$ is projection on i -th component. Note that $\pi_i \in \hat{G}$. Then $x = (x_1, \dots, x_d) = (f(\pi_1), \dots, f(\pi_d)) \in G_m^d$.

Furthermore for $\xi \in \hat{G}$, and let $\iota_i : G_m \rightarrow G_m^d$ be given by

$$\iota_i(x) = (1, \dots, 1, x, 1, \dots, 1) \text{ } x \text{ in } i\text{-th component.}$$

Then

$$\varphi_x(\xi) = \xi(x) = \xi((f(\pi_1), \dots, f(\pi_d))) = \xi\left(\prod_{i=1}^d \iota_i(f(\pi_i))\right) = \prod_{i=1}^d \xi \iota_i(f(\pi_i))$$

On the other hand,

$$f(\xi) = f(\xi \circ \left(\prod_{i=1}^d \iota_i \circ \pi_i\right)) = \prod_{i=1}^d f(\xi \circ \iota_i \circ \pi_i)$$

But $\xi \circ \iota_i : G_m \rightarrow G_m$, corresponds to an integer $n_{\xi,i}$ i.e.

$$\xi \circ \iota_i(x) = x^{n_{\xi,i}}.$$

Therefore we have

$$f(\xi \circ \iota_i \circ \pi_i) = f((\pi_i)^{n_{\xi,i}}) = f(\pi_i)^{n_{\xi,i}} = \xi \circ \iota_i(f(\pi_i))$$

This establishes that

$$f(\xi) = \varphi_{\xi((f(\pi_1), \dots, f(\pi_n)))}(f)$$

i.e. that $x \mapsto \varphi_x$ is surjective for tori.

Proof of (2)

$$A^0 = \{\xi \in \hat{G}, \xi(x) = 1 \text{ for every } x \in A\}$$

$$B^0 = \{x \in G, \xi(x) = 1 \text{ for every } \xi \in B\}$$

If we let $\text{res}_A : \hat{G} \rightarrow \hat{A}$, for a subgroup A of G be the restriction homomorphism, i.e. $\text{res}_A = \hat{\iota}$ where $\iota : A \rightarrow G$ is inclusion homomorphism, then

$$A^0 = \ker \text{res}_A.$$

And

$$B^0 = \bigcap_{\xi \in B} \ker \xi$$

$$(A^0)^0 = \bigcap_{\xi \in A^0} \ker \xi \geq A$$

by definition of A^0 . i.e. $A \leq \ker \xi$ for every $\xi \in A^0$.

$$(B^0)^0 = \ker \text{res}_{B^0} \geq B$$

If $\xi \in B$, then $\text{res}_{B^0}(\xi) = 1$, by definition of B^0 .

We need to show that $\hat{T}/A^0$ is p -torsion free when A is a closed subgroup of T . Recall that in a field of characteristic p , only p th root of unity is one.

We need to show that if $\hat{T}/B$ is p -torsion free then B^0 is a closed subgroup of T .

Proof of (3)

Consider $\pi : T \rightarrow T/A$. then $\hat{\pi} : \widehat{T/A} \rightarrow \hat{T}$. Since π is surjective, $\hat{\pi}$ is injective. But if $\xi \in \text{im } \hat{\pi}$, then $\xi = \hat{\pi}(\xi') = \xi' \circ \pi$ for some $\xi' \in \widehat{T/A}$. Then $\xi(x) = \xi'(\pi(x))$, and for $x \in A$, we have $\xi(x) = \xi'(\pi(x)) = \xi'(1) = 1$, so that $\xi \in A^0$.

So then we have $\widehat{T/A} \cong A^0$.

Consider $\iota : A \rightarrow T$, and $\hat{\iota} : \hat{T} \rightarrow \hat{A}$

If we assume that $\hat{\iota}$ is surjective, then we can argue as follows: If $\xi \in \ker \hat{\iota}$, then $1_{\hat{A}} = \hat{\iota}(\xi) = \xi \circ \iota$, so that for all $x \in A$, we have $\xi \circ \iota(x) = \xi(x) = 1$. i.e. $\xi \in A^0$. Then $\ker \hat{\iota} = A^0$, and

$$\hat{T}/A^0 \cong \hat{A}.$$

Note that $\hat{\iota} = \text{res}_A$. and ι is injective.

We need to show that every rational character of A can be lifted to a rational character of T . If $T \cong AB$ for another subgroup B of T such that $A \cap B = \{1\}$ then this is obvious, by assuming say the character to take the value 1 on B .

On the other hand, one may proceed by considering $A \times T/A$, choosing coset representatives of T/A in A . This may or may not conclude the argument.

Auxiliary Results

Consider $\pi : \hat{T} \rightarrow \hat{T}/B$. then $\hat{\pi} : \widehat{\hat{T}/B} \rightarrow \hat{\hat{T}} \cong \hat{T}$, is injective, since π is surjective. On the other hand if $\varphi_x \in \text{im } \hat{\pi}$, then there exists $\zeta \in \widehat{\hat{T}/B}$, such that $\zeta \circ \pi = \hat{\pi}(\zeta) = \varphi_x$. For any $\xi \in B \leq \hat{T}$, we have $\xi(x) = \varphi_x(\xi) = \zeta \circ \pi(\xi) = \zeta(1) = 1$. But then $x \in B^0$.

So then we have

$$\widehat{\hat{T}/B} \cong B^0.$$

Proof of (4) Recall:

$$\varphi_x(\xi) = \xi(x) \quad \xi \in \hat{G} \quad x \in G$$

$$\hat{\alpha}(\xi') = \xi' \circ \alpha, \quad \xi' \in \hat{G}' \quad \alpha \in \text{Hom}(G, G')$$

Note that for $\alpha \in \text{Hom}(T, T')$ and $x \in T$

$$\hat{\alpha}(x) = \hat{\alpha}(\varphi_x) = \varphi_x \circ \hat{\alpha}$$

Now for $\xi \in \hat{T}'$, we have

$$\varphi_x \circ \hat{\alpha}(\xi) = \varphi_x(\hat{\alpha}(\xi)) = \varphi_x(\xi \circ \alpha) = \xi(\alpha(x)) = \varphi_{\alpha(x)}(\xi)$$

so that we have

$$\varphi_x \circ \hat{\alpha} = \varphi_{\alpha(x)}.$$

So then

$$\hat{\alpha}(\varphi_x) = \varphi_{\alpha(x)}$$

So we can interpret this to mean $\hat{\alpha} = \alpha$, under the identification

$$\hat{\hat{T}} = T$$

Proof of (5)

If α is an isomorphism, then α is surjective, and by lemma, $\hat{\alpha}$ is injective. On the other hand, since $\alpha = \hat{\hat{\alpha}}$, α being injective implies that $\hat{\alpha}$ is surjective. Hence $\hat{\alpha}$ is an isomorphism. If $\hat{\alpha}$ is an isomorphism, then $\alpha = \hat{\hat{\alpha}}$ is also an isomorphism.

Remark (2) and (3) are incomplete. For full proof sources are Grothendieck's article on affine algebraic groups [34] and Borel's article on linear algebraic groups [15].

The result utilizes properties of affine algebraic groups.

8.7.1. Splitting Fields

Definition 173 Let T be a torus defined over a field k . An extension K of k will be called a splitting field of T over k if $\hat{T} = (\hat{T})_K$, where $(\hat{T})_K$ means, according to the convention, the set of characters defined over K . When that is so, we will often say that T splits over K .

Proposition 15 T splits over a finite separable extension of k .

Let $\xi \in \hat{T}$, and Γ_ξ be its graph. Then Γ_ξ is a subtorus of $T \times G_m$, the product defined over k .

The proposition follows from the following lemma:

Lemma 98 Let S be a subtorus of a torus T defined over k . Then S is defined over a finite separable extension of k .

Proposition 16 Let T be a torus over a field k with a splitting field K which is a Galois extension of k , and $\mathfrak{g} = \text{Gal}(K/k)$. The map φ defined by $\varphi_x(\xi) = \xi(x)$ induces the following isomorphisms of $\mathfrak{g}$ -modules:

$$(1) T_K \cong \text{Hom}(T, K^*),$$

$$(2) T_k \cong \text{Hom}_{\mathfrak{g}}(T, K^*).$$

Proposition 17 Let T, T' be tori defined over k and let K be a common splitting field of T, T' which is a finite Galois extension of k . Then $\alpha \mapsto \hat{\alpha}$ defined by $\hat{\alpha}(\xi) = \xi \circ \alpha$ induces an isomorphism: $\text{Hom}_k(T, T') \cong \text{Hom}_{\mathfrak{g}}(\hat{T}', \hat{T})$ where $\text{Hom}_k(T, T')$ means the set of k -homomorphisms of T in T' ; α is a k -isomorphism if and only if $\hat{\alpha}$ is a $\mathfrak{g}$ -isomorphism.

Proposition 18 Let M be a finitely generated torsion free $\mathfrak{g}$ -module. Then there exists one and only one torus T defined over k , up to a k -isomorphism, such that T splits over K and that $\hat{T} \cong M$ as $\mathfrak{g}$ -modules.

8.8. CHARACTERS OF MULTIPLICATIVE GROUP

Lemma 99 If $f : K^* \rightarrow K^*$ is a multiplicative function, i.e. $f(xy) = f(x)f(y)$ and f is smooth, then $f(x) = x^a$ where $a = f'(1)$ here $K = \mathbb{R}$ or $K = \mathbb{C}$

Proof. First note $f(x) = f(x)f(1)$ Since $f(x) \neq 0$ $f(1) = 1$. Treating y as a constant in the equation

$$f(xy) = f(x)f(y)$$

and differentiating with respect to x gives

$$yf'(xy) = f(y)f'(x)$$

Setting $x = 1$ gives

$$yf'(y) = f(y)f'(1)$$

i.e.

$$\frac{f'(y)}{f(y)} = \frac{f'(1)}{y}$$

Then assuming $f(y)$ is in a region where logarithm is defined,

$$\frac{d}{dy} \ln f(y) = \frac{d}{dy} (f'(1) \ln y)$$

or

$$\frac{d}{dy} \ln \frac{f(y)}{y^{f'(1)}} = 0$$

Hence $f(y) = \kappa y^{f'(1)}$ where κ is a constant. Setting $y = 1$ gives $\kappa = 1$. Note also, $y^\alpha = \exp(\alpha \ln y)$ and for this function to be defined on the whole complex plane with no cuts, α has to be an integer, in which case we don't need to use this expression.

Now note

$$\frac{f(xy) - f(x)}{xy - x} = \frac{f(x)(f(y) - 1)}{x(y - 1)} = \frac{f(x)}{x} \frac{f(y) - 1}{y - 1}$$

If $\lim_{y \rightarrow 1} \frac{f(y)-1}{y-1}$ exists, then the function is differentiable everywhere, and this condition is equivalent to the function being differentiable at identity 1.

Now in some setting a character of an algebraic group is defined as follows:

Definition 174 A character of an algebraic group G is any morphism of algebraic groups $\chi : G \rightarrow \mathbb{G}_m$ where $\mathbb{G}_m$ is the multiplicative group of the field over which the algebraic

group is defined. Characters can be multiplied, and they form an abelian group denoted by $X(G)$. Character group $X(G)$ is a subset of the K -algebra $K[G]$, the coordinate ring of G , where G is an algebraic group over K . ($K[G]$ can refer to the K -algebra generated on G .)

Now since characters are defined by morphism of algebraic groups, they are rational functions of the coordinates on the algebraic group, hence are differentiable functions. Of course the lemma above with differentiation works over the complete field, but there is no reason why it should not work on any finite extension of $\mathbb{Q}$. or even with p -adics.

In other words $X(\mathbb{G}_m(K)) = \mathbb{Z}$ when $\text{char}(K) = 0$.

8.9. CONSTRUCTION OF SERRE-TANIYAMA GROUP

Starting with the exact sequence

$$1 \longrightarrow K^*/E_m \longrightarrow I_m \longrightarrow C_m \longrightarrow 1$$

And the map $K^*/E_m \rightarrow T_m$ where $T_m = T/\bar{E}_m$ and T is the torus $R_{K/\mathbb{Q}}(G_{m/K})$ and closure is Zariski closure in T . the theorem previously quoted in the enlarging groups section yields a short exact sequence and commutative diagram.

Note $\pi_{H,K}^G : G/H \rightarrow G/K$ is defined when $H \leq K$, by $\pi(gH) = gK$. Since if $g' \in gH$, then $g' \in gK$, this map is well-defined. Now take $G = K^*$ and $H = E_m$, and $K = \bar{E}_m$. Then note that K^* is isomorphic to $R_{K/\mathbb{Q}}(G_{m/K})$.

Now if we consider the group homomorphism $K^*/E_m \rightarrow T_m = T/\bar{E}_m$, by the theorem proved in the section Enlarging Group, we obtain an algebraic group S_m (over $\mathbb{Q}$), a group homomorphism $\epsilon_m : I_m \rightarrow S_m(\mathbb{Q})$, and the commutative diagram of exact sequences:

$$\begin{array}{ccccccc} 1 & \longrightarrow & K^*/E_m & \longrightarrow & I_m & \longrightarrow & C_m \longrightarrow 1 \\ & & \downarrow & & \downarrow \epsilon_m & & \downarrow \text{id} \\ 1 & \longrightarrow & T_m(\mathbb{Q}) & \longrightarrow & S_m(\mathbb{Q}) & \longrightarrow & C_m \longrightarrow 1 \end{array}$$

Note also that the homomorphism $K^*/E_m \rightarrow T_m(\mathbb{Q})$ is surjective.

Lemma 100 Kernel of $\epsilon_m : I_m \rightarrow S_m(\mathbb{Q})$ is the image of $\bar{E}_m$ under $K^* \rightarrow I_m$.

Note that $\ker \epsilon_m \subset \ker(I_m \rightarrow C_m) = \text{im } K^*/E_m \rightarrow I_m$, by exactness. By commutativity of the diagram of exact sequences, an element in $\ker \epsilon_m$ when pulled back to K^*/E_m must be mapped to zero in $T_m(\mathbb{Q})$ since $T_m(\mathbb{Q}) \rightarrow S_m(\mathbb{Q})$ is injective. But the kernel of $K^*/E_m \rightarrow T_m(\mathbb{Q})$, by definition of this map, is $\bar{E}_m/E_m$.

The following is stated in [84] II-8,9.

Theorem 22 *The algebraic groups S_m form a projective system, whose projective limit is a proalgebraic group over $\mathbb{Q}$ which is the extension of the profinite group $C/D = \varprojlim_m C_m$ by a torus $\varprojlim_m T_m$.*

Remark By class field theory, $C/D \cong \text{Gal}(K^{\text{ab}}/\mathbb{Q}) \cong \text{Gal}(K/\mathbb{Q})^{\text{ab}}$.

For a modulus m with support S_m and modulus n with support S_n , define $m \leq n$ to mean that:

- (i) $S_m \subset S_n$.
- (ii) $m_v \leq n_v$ for each $v \in S_m$.

Note that if $m \leq n$, then $U_n \subset U_m$. Recall

$$U_m = \prod_{v \in \Sigma_K^\infty} K_v^o \times \prod_{v \in S_m} (1 + \mathfrak{m}_v^{m_v}) \times \prod_{v \in \Sigma_K - S} U_v$$

where K_v^o is the connected component of identity in K_v^* , and $\mathfrak{m}_v$ is the maximal ideal of the valuation field K_v .

If $n_v \geq m_v$, then $(1 + \mathfrak{m}_v^{n_v}) \subset (1 + \mathfrak{m}_v^{m_v})$, for $v \in S_m$.

If $v \in S_n - S_m$, then $(1 + \mathfrak{m}_v^{n_v}) \subset U_v$.

But then, we obtain morphisms $I/U_n \rightarrow I/U_m$ is surjective, $K^*/E_n \rightarrow K^*/E_m$ surjective, $C_n = I/K^*U_n \rightarrow C_m = I/K^*U_m$, which result in surjective morphisms $T_n \rightarrow T_m$, $S_n \rightarrow S_m$ and $C_n \rightarrow C_m$, to give the following commutative diagram:

$$\begin{array}{ccccccc}
& & 1 & \longrightarrow & T_n(\mathbb{Q}) & \longrightarrow & S_n(\mathbb{Q}) \longrightarrow C_n \longrightarrow 1 \\
& & & \nearrow & \epsilon_n \nearrow & & \text{id} \nearrow \\
1 & \longrightarrow & K^*/E_n & \longrightarrow & I_n & \longrightarrow & C_n \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & K^*/E_m & \longrightarrow & I_m & \longrightarrow & C_m \longrightarrow 1 \\
& & \searrow & & \epsilon_m \searrow & & \text{id} \searrow \\
& & 1 & \longrightarrow & T_m(\mathbb{Q}) & \longrightarrow & S_m(\mathbb{Q}) \longrightarrow C_m \longrightarrow 1
\end{array}$$

By considering this diagram, and the kernels of the morphisms, we see that this diagram can be completed to a full commutative diagram with morphisms from $T_n \rightarrow T_m$, $S_n \rightarrow S_m$, and $C_n \rightarrow C_m$, which are all surjective.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & K^*/E_n & \longrightarrow & I_n & \longrightarrow & C_n & \longrightarrow & 1 \\
& & \downarrow & \searrow & \downarrow & \searrow \epsilon_n & \downarrow & \searrow \text{id} & \\
& & 1 & \longrightarrow & T_n(\mathbb{Q}) & \longrightarrow & S_n(\mathbb{Q}) & \longrightarrow & C_n \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & K^*/E_m & \longrightarrow & I_m & \longrightarrow & C_m & \longrightarrow & 1 \\
& & \searrow & & \epsilon_m \searrow & & \text{id} \searrow & & \\
& & 1 & \longrightarrow & T_m(\mathbb{Q}) & \longrightarrow & S_m(\mathbb{Q}) & \longrightarrow & C_m \longrightarrow 1
\end{array}$$

Surjectivity together with Mittag-Leffler condition suffices to conclude that this projective system gives rise to an exact sequence of groups which are projective limits of the groups in consideration.

It only needs to be argued that projective limit of tori T_m is a torus.

Definition 175 An inverse system (A_n) of sets with connecting maps $u_{m,n} : A_m \rightarrow A_n$ for $m \geq n$ is said to satisfy Mittag-Leffler condition if for each n , the decreasing sequence $u_{m,n}(A_m)$ ($m \geq n$) stabilizes, i.e. is constant for sufficiently large m .

Lemma 101 This condition is satisfied when $u_{m,n}$ is surjective for all m, n .

Proposition 19 If an inverse system (A_n) satisfies Mittag-Leffler condition, and for each

$n, \quad 0 \longrightarrow A_n \longrightarrow B_n \longrightarrow C_n \longrightarrow 0$ is an exact sequence with connecting maps being compatible with exact sequences, then sequence formed of the projective limits is also an exact sequence.

Source: [59] pp 164.

8.10. GROUP COHOMOLOGY RESULTS

Lemma 102 *If A is an abelian group, and E is an extension of G by A , i.e. there is an exact sequence*

$$1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1$$

meaning that ι is injective, π is surjective, and $\ker \pi = \text{im } \iota$, then for any section $a : G \rightarrow E$, (that means any map such that $\pi \circ a = \text{id}$), then

(1) *G acts on A by inner conjugation in E i.e.*

$$g(x) = a(g)xa(g)^{-1}$$

defines a group action of G on A , independent of section,

(2) *the function*

$$d : G \times G \rightarrow A$$

defined by

$$d_{g,h} = d(g, h) = a(g)a(h)a(gh)^{-1}$$

satisfies

$$\tau_1(d_{\tau_2, \tau_3})d_{\tau_1, \tau_2 \tau_3} = d_{\tau_1, \tau_2}d_{\tau_1 \tau_2, \tau_3}$$

Note d measures the failure of section a to be a homomorphism, and is always equal to identity of the group if and only if a is a homomorphism.

Action is independent of section chosen: Since $\ker \pi = \iota(A)$, we have that $\iota(A)$ is a normal subgroup of E , so that $gx \in A$, whenever $x \in A$.

If $a' : G \rightarrow E$ is another section, then we have

$$f(g) = a(g)^{-1}a'(g) \in A,$$

defines a function $f : G \rightarrow A$. Since $\pi(a(g)) = g = \pi(a'(g))$, we have that $\pi(f(g)) = e_G$, hence $f(g) \in \ker \pi = \iota(A)$. Then

$$a'(g)xa'(g)^{-1} = a(g)f(g)x(a(g)f(g))^{-1} = a(g)f(g)xf(g)^{-1}a(g)^{-1} = a(g)xa(g)^{-1}$$

where we utilize that A is abelian, hence $f(g)xf(g)^{-1} = x$ whenever $x \in A$.

That $d_{-, -} \in A$

$$\pi(a(g)a(h)a(gh)^{-1}) = \pi(a(g))\pi(a(h))\pi(a(gh))^{-1} = gh(gh)^{-1} = gh h^{-1}g^{-1} = e_G,$$

hence $d_{g,h} \in \ker \pi = \iota(A)$.

Group Action

Use the notation $\mathcal{A}(g, x) = g(x) = a(g)xa(g)^{-1}$.

$\mathcal{A}(e_G, x) = a(e_G)xa(e_G)^{-1}$, and because $a(e_G) \in A$, and A is abelian, we have that $\mathcal{A}(e_G, x) = x$.

$$\begin{aligned} \mathcal{A}(g, \mathcal{A}(h, x)) &= \mathcal{A}(g, a(h)xa(h)^{-1}) \\ &= a(g)a(h)xa(h)^{-1}a(g)^{-1} \\ &= a(g)a(h)xa(h)^{-1}a(g)^{-1} \\ &= d_{g,h}a(gh)xa(gh)^{-1}d_{g,h}^{-1} \\ &= d_{g,h}\mathcal{A}(gh, x)d_{g,h}^{-1} \\ &= \mathcal{A}(gh, x) \end{aligned}$$

where we utilize that $d_{-, -}$ lies in A and $\mathcal{A}(-, x)$ lies in A for $x \in A$, and that A is abelian, to conclude that conjugation by $d(g, h)$ leaves $\mathcal{A}(-, x)$ invariant.

Equation satisfied by $d_{-, -}$

$$\begin{aligned}
 d_{\tau_1, \tau_2} d_{\tau_1 \tau_2, \tau_3} &= a(\tau_1) a(\tau_2) a(\tau_1 \tau_2)^{-1} a(\tau_1 \tau_2) a(\tau_3) a(\tau_1 \tau_2 \tau_3)^{-1} \\
 &= a(\tau_1) a(\tau_2) a(\tau_3) a(\tau_1 \tau_2 \tau_3)^{-1} \\
 &= a(\tau_1) d_{\tau_2, \tau_3} a(\tau_2 \tau_3) a(\tau_1 \tau_2 \tau_3)^{-1} \\
 &= a(\tau_1) d_{\tau_2, \tau_3} a(\tau_1)^{-1} a(\tau_1) a(\tau_2 \tau_3) a(\tau_1 \tau_2 \tau_3)^{-1} \\
 &= a(\tau_1) d_{\tau_2, \tau_3} a(\tau_1)^{-1} d_{\tau_1, \tau_2 \tau_3} \\
 &= \tau_1 (d_{\tau_2, \tau_3}) d_{\tau_1, \tau_2 \tau_3}
 \end{aligned}$$

where we have used the definition of $d_{-, -}$, and the definition for action of G on A by inner conjugation.

8.10.1. Different Sections

Lemma 103 *Let $\mathcal{A}$ denote the action of G on A as in previous lemma. Above if d^1 and d^2 are the functions corresponding to sections a^1 and a^2 , then*

$$d^2(g, h) = \mathcal{A}(g, f(g)) \mathcal{A}(gh, f(h) f(gh)^{-1}) d^1(g, h)$$

for $f(g) = f^1(g) = a^1(g)^{-1} a^2(g)$ OR

$$d^2(g, h) = f(g) \mathcal{A}(g, f(h)) f(gh)^{-1} d^1(g, h)$$

for $f(g) = f^2(g) = a^2(g) a^1(g)^{-1}$ Furthermore the choices are related by

$$\mathcal{A}(g, f^1(g)) = f^2(g)$$

Here $f : G \rightarrow A$

CHOICES for $f(g)$

$$(1) f(g) = a^2(g)a^1(g)^{-1}$$

$$(2) f(g) = a^1(g)^{-1}a^2(g)$$

$$(3) f(g) = a^1(g)a^2(g)^{-1} \text{ inverse of first choice, swap 1 and 2 in first choice}$$

$$(4) f(g) = a^2(g)^{-1}a^1(g) \text{ inverse of second choice, swap 1 and 2 in second choice}$$

CHOICES for $e(g, h)$

$$(1) e(g, h) = d^2(g, h)d^1(g, h)^{-1}$$

$$(2) e(g, h) = d^1(g, h)^{-1}d^2(g, h)$$

$$(3) e(g, h) = d^1(g, h)d^2(g, h)^{-1} \text{ inverse of first choice, swap 1 and 2 in first choice}$$

$$(4) e(g, h) = d^2(g, h)^{-1}d^1(g, h) \text{ inverse of second choice, swap 1 and 2 in second choice}$$

Transitions between choices:

$$xy = [x, y]yx$$

so

$$a^2(g)a^1(g)^{-1} = [a^2(g), a^1(g)^{-1}]a^1(g)^{-1}a^2(g)$$

Furthermore, $[a^2(g), a^1(g)^{-1}] \in A$.

Since $d^i(g, h) \in A$, the choices for e do not matter, the terms commute.

Choice (2,3) Let $e_{g,h} = e(g, h) = d^1(g, h)d^2(g, h)^{-1} \in A$ and $f(g) = a^1(g)^{-1}a^2(g) \in A$.

Then

$$\begin{aligned}
e_{g,h} &= (a^1(g)a^1(h)a^1(gh)^{-1}) (a^2(g)a^2(h)a^2(gh)^{-1})^{-1} \\
&= (a^1(g)a^1(h)a^1(gh)^{-1}) (a^2(gh)a^2(h)^{-1}a^2(g)^{-1}) \\
&= (a^1(g)a^1(h)) (a^1(gh)^{-1}a^2(gh)) (a^2(h)^{-1}a^2(g)^{-1}) \\
&= (a^1(g)a^1(h)) (f(gh)) (a^2(h)^{-1}a^2(g)^{-1}) \\
&= (a^1(g)a^1(h)) (f(gh)) (a^1(g)a^1(h))^{-1} (a^1(g)a^1(h)) (a^2(h)^{-1}a^2(g)^{-1}) \\
&= (a^1(g)a^1(h)) (f(gh)) (a^1(h)^{-1}a^1(g)^{-1}) (a^1(g)a^1(h)) (a^2(h)^{-1}a^2(g)^{-1}) \\
&= \mathcal{A}(g, \mathcal{A}(h, f(gh))) (a^1(g)a^1(h)) (a^1(h)f(h))^{-1} (a^1(g)f(g))^{-1} \\
&= \mathcal{A}(gh, f(gh)) (a^1(g)a^1(h)) (f(h)^{-1}a^1(h)^{-1}) (f(g)^{-1}a^1(g)^{-1}) \\
&= \mathcal{A}(gh, f(gh)) (a^1(g)a^1(h)f(h)^{-1}a^1(h)^{-1}) f(g)^{-1}a^1(g)^{-1} \\
&= \mathcal{A}(gh, f(gh))\mathcal{A}(g, \mathcal{A}(h, f(h)^{-1})f(g)^{-1}) \\
&= \mathcal{A}(gh, f(gh))\mathcal{A}(gh, f(h)^{-1})\mathcal{A}(g, f(g)^{-1}) \\
&= \mathcal{A}(gh, f(gh)f(h)^{-1})\mathcal{A}(g, f(g)^{-1})
\end{aligned}$$

SO

$$e_{g,h}^{-1} = \mathcal{A}(g, f(g))\mathcal{A}(gh, f(h)f(gh)^{-1})$$

For alternate equation, this time let $e_{g,h} = d^1(g, h)^{-1}d^2(g, h)$

$$\begin{aligned}
 e_{g,h} &= (a^1(g)a^1(h)a^1(gh)^{-1})^{-1} (a^2(g)a^2(h)a^2(gh)^{-1}) \\
 &= (a^1(gh)a^1(h)^{-1}) (a^1(g)^{-1}a^2(g)) (a^2(h)a^2(gh)^{-1}) \\
 &= (a^1(gh)a^1(h)^{-1}) (f(g)) (a^2(h)a^2(gh)^{-1}) \\
 &= a^1(gh)(a^1(h)^{-1}f(g)a^1(h))(a^1(h)^{-1}a^2(h))a^2(gh)^{-1} \\
 &= a^1(gh)\mathcal{A}(h^{-1}, f(g))f(h)a^2(gh)^{-1} \\
 &= a^1(gh)\mathcal{A}(h^{-1}, f(g))f(h)(a^1(gh)f(gh))^{-1} \\
 &= a^1(gh)\mathcal{A}(h^{-1}, f(g))f(h)f(gh)^{-1}a^1(gh)^{-1} \\
 &= \mathcal{A}(gh, \mathcal{A}(h^{-1}, f(g))f(h)f(gh)^{-1}) \\
 &= \mathcal{A}(gh, \mathcal{A}(h^{-1}, f(g)))\mathcal{A}(gh, f(h)f(gh)^{-1}) \\
 &= \mathcal{A}(gh, \mathcal{A}(h^{-1}, f(g)))\mathcal{A}(gh, f(h)f(gh)^{-1}) \\
 &= \mathcal{A}(g, f(g))\mathcal{A}(gh, f(h)f(gh)^{-1})
 \end{aligned}$$

Choice (1,4) this time assume $f(g) = a^2(g)a^1(g)^{-1}$,

$$\begin{aligned}
 d^1(g, h)f(g)\mathcal{A}(g, f(h)) &= d^1(g, h)a^2(g)a^1(g)^{-1}a^1(g)a^2(h)a^1(h)^{-1}a^1(g)^{-1} \\
 &= d^1(g, h)a^2(g)a^2(h)a^2(gh)^{-1}a^2(gh)a^1(h)^{-1}a^1(g)^{-1} \\
 &= d^1(g, h)d^2(g, h)a^2(gh)a^1(gh)^{-1}a^1(gh)a^1(h)^{-1}a^1(g)^{-1} \\
 &= d^1(g, h)d^2(g, h)f(gh)d^1(g, h)^{-1} \\
 &= d^2(g, h)f(gh)
 \end{aligned}$$

$$\begin{aligned}
 d^2(g, h)^{-1}d^1(g, h) &= (a^2(g)a^2(h)a^2(gh)^{-1})^{-1}a^1(g)a^1(h)a^1(gh)^{-1} \\
 &= a^2(gh)a^2(h)^{-1}a^2(g)^{-1}a^1(g)a^1(h)a^1(gh)^{-1} \\
 &= f(gh)a^1(gh)(f(h)a^1(h))^{-1}(f(g)a^1(g))^{-1}a^1(g)a^1(h)a^1(gh)^{-1} \\
 &= f(gh)a^1(gh)a^1(h)^{-1}f(h)^{-1}a^1(g)^{-1}f(g)^{-1}a^1(g)a^1(h)a^1(gh)^{-1} \\
 &= f(gh)\mathcal{A}(gh, \mathcal{A}(h^{-1}, f(h)^{-1}\mathcal{A}(g^{-1}, f(g)^{-1}))) \\
 &= f(gh)\mathcal{A}(ghh^{-1}, f(h)^{-1}\mathcal{A}(g^{-1}, f(g)^{-1})) \\
 &= f(gh)\mathcal{A}(g, f(h)^{-1})\mathcal{A}(gg^{-1}, f(g)^{-1}) \\
 &= f(gh)\mathcal{A}(g, f(h)^{-1})f(g)^{-1}
 \end{aligned}$$

i.e. $d^1(g, h)^{-1}d^2(g, h) = f(g)\mathcal{A}(g, f(h))f(gh)^{-1}$

If we name the following elements in A as follows:

$$f^2(g) = a^1(g)^{-1}a^2(g) \text{ and } f^1(g) = a^2(g)a^1(g)^{-1} \text{ and } t(g) = [a^1(g), a^2(g)^{-1}]$$

so that $f^1(g)t(g) = f^2(g)$ then we have

$$d^2(g, h)d^1(g, h)^{-1} = \mathcal{A}(g, f^2(g))\mathcal{A}(gh, f^2(h))f^2(gh)^{-1}$$

and

$$d^1(g, h)^{-1}d^2(g, h) = f^1(g)\mathcal{A}(g, f^1(h))f^1(gh)^{-1}$$

Note the property:

$$\begin{aligned} \mathcal{A}(g, f^1(g)) &= \mathcal{A}(g, a^1(g)^{-1}a^2(g)) \\ &= a^1(g)a^1(g)^{-1}a^2(g)a^1(g)^{-1} \\ &= a^2(g)a^1(g)^{-1} \\ &= f^2(g) \end{aligned}$$

so that $\mathcal{A}(g, f^1(g)) = f^2(g)$

Using this property we get:

$$\begin{aligned}
 & \mathcal{A}(g, f^1(g))\mathcal{A}(gh, f^1(h)f^1(gh)^{-1}) \\
 &= \mathcal{A}(g, f^1(g))\mathcal{A}(gh, f^1(h))\mathcal{A}(gh, f^1(gh))^{-1} \\
 &= \mathcal{A}(g, f^1(g))\mathcal{A}(g, \mathcal{A}(h, f^1(h)))\mathcal{A}(gh, f^1(gh))^{-1} \\
 &= f^2(g)\mathcal{A}(g, f^2(h))(f^2(gh))^{-1}
 \end{aligned}$$

that the two equations are identical.

8.10.2. Further Lemmas

Lemma 104 (*Semidirect products*) *Given a group A and a group G that acts on A , there exists a group E , group homomorphisms $\iota : A \rightarrow E$ and $\pi : E \rightarrow G$ such that the sequence*

$$1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1$$

is exact, and if A is abelian, then

$$\iota(\pi(x)(a)) = x\iota(a)x^{-1}$$

for any $x \in E$, and $a \in A$. Furthermore there exists a group homomorphism $s : G \rightarrow E$, such that $\pi(s(g)) = g$, i.e. the sequence is split exact.

Remark If we let $d(g, h) = s(g)s(h)s(gh)^{-1}$ then note that for s a homomorphism, $d : G \times G \rightarrow A$ is the constant function $d(g, h) = e_A$.

Construction of E

Let $E = A \times G$ as a set. Define group operation on E by the rule:

$$(a_1, g_1)(a_2, g_2) = (a_1g_1(a_2), g_1g_2)$$

Group Properties :

Associativity

$$\begin{aligned}
 ((a_1, g_1)(a_2, g_2))(a_3, g_3) &= (a_1 g_1(a_2), g_1 g_2)(a_3, g_3) \\
 &= ((a_1 g_1(a_2))(g_1 g_2)(a_3), (g_1 g_2)g_3)
 \end{aligned}$$

$$\begin{aligned}
 (a_1, g_1)((a_2, g_2)(a_3, g_3)) &= (a_1, g_1)(a_2 g_2(a_3), g_2 g_3) \\
 &= (a_1 g_1(a_2 g_2(a_3)), g_1(g_2 g_3)) \\
 &= (a_1(g_1(a_2)(g_1 g_2)(a_3)), g_1(g_2 g_3))
 \end{aligned}$$

Unit

It can be verified that (e_A, e_G) is a unit of this operation.

Inverse Solving the equation

$$(a_1, g_1)(a_2, g_2) = (e_A, e_G)$$

i.e.

$$(a_1 g_1(a_2), g_1 g_2) = (e_A, e_G)$$

we get: $g_2 = g_1^{-1}$ and $a_2 = g_1^{-1}(a_1^{-1})$ or $g_1 = g_2^{-1}$ and $a_1 = (g_1(a_2))^{-1} = g_2^{-1}(a_2^{-1})$

Therefore

$$(a, g)^{-1} = (g^{-1}(a^{-1}), g^{-1})$$

Group homomorphisms and Exact Sequence

Now note that $\iota : A \rightarrow E$ defined by $\iota(a) = (a, e_G)$ is a group homomorphism:

$$\begin{aligned}\iota(a_1)\iota(a_2) &= (a_1, e_G)(a_2, e_G) \\ &= (a_1e_G(a_2), e_G) \\ &= (a_1a_2, e_G) \\ &= \iota(a_1a_2)\end{aligned}$$

It is clear that ι is injective.

$\pi : E \rightarrow G$ defined by $\pi((a, g)) = g$ is a group homomorphism:

$$\begin{aligned}\pi((a_1, g_1)(a_2, g_2)) &= \pi((a_1g_1(a_2), g_1g_2)) \\ &= g_1g_2 \\ &= \pi((a_1, g_1))\pi((a_2, g_2))\end{aligned}$$

Since $\pi((e_A, g)) = g$ for any $g \in G$, π is surjective.

It is clear that $\iota(A) = \{(a, e_G) \mid a \in A\} = \ker \pi$ since $\pi((a, g)) = e_G$ if and only if $g = e_G$.

Group action and inner conjugation

$$\begin{aligned}(b, g)(a, e_G)(b, g)^{-1} &= (bg(a), g)(g^{-1}(b^{-1}), g^{-1}) \\ &= (bg(a)g(g^{-1}(b^{-1})), gg^{-1}) \\ &= (bg(a)b^{-1}, e_G)\end{aligned}$$

Hence

$$(b, g)(a, e_G)(b, g)^{-1} = (bg(a)b^{-1}, e_G)$$

If A is abelian, then $bg(a)b^{-1} = g(a)$, so that

$$(b, g)(a, e_G)(b, g)^{-1} = (g(a), e_G)$$

Splitness

Let $s : G \rightarrow E$ be defined by $s(g) = (e_A, g)$. Then we have

$$s(g)s(h) = (e_A, g)(e_A, h) = (e_Ag(e_A), gh) = (e_A, gh) = s(gh)$$

This is a homomorphism, and is injective. Clearly $\pi(s(g)) = g$.

Lemma 105 (*Existence of extension and section compatible with d*) Given an abelian group A and a group G that acts on A and a function $d : G \times G \rightarrow A$, that satisfies:

$$\tau_1(d_{\tau_2, \tau_3})d_{\tau_1, \tau_2 \tau_3} = d_{\tau_1, \tau_2}d_{\tau_1 \tau_2, \tau_3}$$

for $\tau_1, \tau_2, \tau_3 \in G$, there exists a group E , and group homomorphisms $\iota : A \rightarrow E$ and $\pi : E \rightarrow G$ such that the sequence

$$1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1$$

is exact.

Furthermore there exists a map $s : G \rightarrow E$ such that $\pi(s(g)) = g$ (i.e. a section) such that

$$d(g, h) = s(g)s(h)s(gh)^{-1}$$

The action of G on A coincides with inner conjugation by a section. i.e.

$$s(g)\iota(x)s(g)^{-1} = \iota(g(x))$$

for $g \in G$ and $x \in A$ and $g(x)$ denotes the action of g on x .

Group Construction

Let $E = A \times G$ as a set. Define operation on E by

$$(a_1, g_1)(a_2, g_2) = (a_1g_1(a_2)d_{g_1, g_2}, g_1g_2)$$

Group Properties

Associativity

$$\begin{aligned} ((a_1, g_1)(a_2, g_2))(a_3, g_3) &= (a_1g_1(a_2)d(g_1, g_2), g_1g_2)(a_3, g_3) \\ &= ((a_1g_1(a_2))d(g_1, g_2)(g_1g_2)(a_3)d(g_1g_2, g_3), (g_1g_2)g_3) \end{aligned}$$

$$\begin{aligned} (a_1, g_1)((a_2, g_2)(a_3, g_3)) &= (a_1, g_1)(a_2g_2(a_3)d(g_2, g_3), g_2g_3) \\ &= (a_1g_1(a_2g_2(a_3)d(g_2, g_3))d(g_1, g_2g_3), g_1(g_2g_3)) \\ &= (a_1(g_1(a_2)(g_1g_2)(a_3)g_1(d(g_2, g_3))d(g_1, g_2g_3)), g_1(g_2g_3)) \end{aligned}$$

The condition for associativity to hold is

$$(a_1g_1(a_2))d(g_1, g_2)(g_1g_2)(a_3)d(g_1g_2, g_3) = a_1(g_1(a_2)(g_1g_2)(a_3)g_1(d(g_2, g_3))d(g_1, g_2g_3))$$

in the first coordinate. Eliminating the same initial terms:

$$d(g_1, g_2)(g_1g_2)(a_3)d(g_1g_2, g_3) = (g_1g_2)(a_3)g_1(d(g_2, g_3))d(g_1, g_2g_3)$$

which can be rearranged as:

$$((g_1g_2)(a_3))^{-1}d(g_1, g_2)(g_1g_2)(a_3)d(g_1g_2, g_3)d(g_1, g_2g_3)^{-1} = g_1(d(g_2, g_3))$$

Utilizing the abelianness of A , inner conjugation by an element of A is the same term:

$$d(g_1, g_2)d(g_1g_2, g_3)d(g_1, g_2g_3)^{-1} = g_1(d(g_2, g_3))$$

i.e.

$$d(g_1, g_2)d(g_1g_2, g_3) = g_1(d(g_2, g_3))d(g_1, g_2g_3)$$

But this is the condition that the function d satisfies.

Unit

The result of this section is:

the unit element is given by

$$(d_{e_G, e_G}^{-1}, e_G)$$

Start with the condition for an element to be a unit (left and right unit separately).

$$(a_1, g_1)(a_2, g_2) = (a_1g_1(a_2)d_{g_1, g_2}, g_1g_2) = (a_i, g_i)$$

for $i = 1, 2$ on right hand side determines the unit.

$a_1g_1(a_2)d_{g_1, g_2} = a_1$ and $g_1g_2 = g_1$ gives that $g_2 = e_G$, and $g_1(a_2)d_{g_1, g_2} = e_A$, hence $a_2 = g_1^{-1}(d_{g_1, g_2}^{-1}) = g_1^{-1}(d_{g_1, e_G}^{-1})$

On the other hand, $a_1g_1(a_2)d_{g_1, g_2} = a_2$ and $g_1g_2 = g_2$ gives that $g_1 = e_G$ and $a_1 = a_2d_{g_1, g_2}^{-1}g_1(a_2^{-1}) = a_2d_{e_G, g_2}^{-1}a_2^{-1}$ by commutativity of A this is equal to d_{e_G, g_2}^{-1} .

We can not be sure at this point that these are units, because in this form they seem to depend on the elements, but a unit element is fixed, not changing with respect to the elements being operated upon. However:

$$d(g_1, g_2)d(g_1g_2, g_3) = g_1(d(g_2, g_3))d(g_1, g_2g_3)$$

setting $g_1 = e_G$ gives

$$d(e_G, g_2)d(g_2, g_3) = d(g_2, g_3)d(e_G, g_2g_3)$$

By abelianness of A $d(g_2, g_3)$ can be cancelled to give:

$$d(e_G, g_2) = d(e_G, g_2g_3)$$

Setting $g_2 = e_G$ gives:

$$d(e_G, e_G) = d(e_G, g_3) \quad [*1]$$

Setting $g_2 = g_3 = e_G$ in the initial equation gives:

$$d(g_1, e_G)d(g_1, e_G) = g_1(d(e_G, e_G))d(g_1, e_G)$$

$d(g_1, e_G)$ can be cancelled to give:

$$d(g_1, e_G) = g_1(d(e_G, e_G)) \quad [*2]$$

i.e.

$$g_1^{-1}(d(g_1, e_G)) = d(e_G, e_G)$$

Therefore in the first case: $g_1^{-1}(d_{g_1, e_G}^{-1}) = (g_1^{-1}(d_{g_1, e_G}))^{-1} = d(e_G, e_G)^{-1}$ and in the second case: $d_{e_G, g_2}^{-1} = d_{e_G, e_G}^{-1}$ Hence dependence on terms is gone, and the unit element is given by

$$(d_{e_G, e_G}^{-1}, e_G)$$

In fact:

$$\begin{aligned}
 (a, g)(d_{e_G, e_G}^{-1}, e_G) &= (ag(d_{e_G, e_G}^{-1})d_{g, e_G}, g) \\
 &= (ag(d_{e_G, e_G})^{-1}d_{g, e_G}, g) \\
 &= (ag(d_{e_G, e_G})^{-1}d_{g, e_G}, g) \\
 &= (ad_{g, e_G}^{-1}d_{g, e_G}, g) \\
 &= (a, g)
 \end{aligned}$$

by [*2]

and

$$\begin{aligned}
 (d_{e_G, e_G}^{-1}, e_G)(a, g) &= (d_{e_G, e_G}^{-1}e_G(a)d_{e_G, g}, g) \\
 &= (d_{e_G, e_G}^{-1}ad_{e_G, g}, g) \\
 &= (ad_{e_G, e_G}^{-1}d_{e_G, g}, g) \\
 &= (a, g)
 \end{aligned}$$

By abelianness of A and [*1]

Inverse

Result of this section is that the inverse is given by

$$(a, g)^{-1} = (d_{e_G, e_G}^{-1}d_{g^{-1}, g}^{-1}g^{-1}(a^{-1}), g^{-1}).$$

Suppose

$$(a_1, g_1)(a_2, g_2) = (d_{e_G, e_G}^{-1}, e_G),$$

i.e.

$$(a_1 g_1(a_2) d_{g_1, g_2}, g_1 g_2) = (d_{e_G, e_G}^{-1}, e_G)$$

This gives two separate equations:

$$a_1 g_1(a_2) d_{g_1, g_2} = d_{e_G, e_G}^{-1} \quad \text{and} \quad g_1 g_2 = e_G$$

Hence

$$a_1 = d_{e_G, e_G}^{-1} d_{g_1, g_2}^{-1} g_1(a_2^{-1}) \quad \text{and} \quad g_1 = g_2^{-1},$$

i.e.

$$a_1 = d_{e_G, e_G}^{-1} d_{g_2^{-1}, g_2}^{-1} g_2^{-1}(a_2^{-1}) \quad \text{and} \quad g_1 = g_2^{-1}$$

In other direction:

$$a_2 = g_1^{-1}(a_1^{-1} d_{e_G, e_G}^{-1} d_{g_1, g_1^{-1}}^{-1}) \quad \text{and} \quad g_2 = g_1^{-1}$$

In the equation satisfied by d

$$d(g_1, g_2) d(g_1 g_2, g_3) = g_1(d(g_2, g_3)) d(g_1, g_2 g_3)$$

setting $g_1 = g$, $g_2 = g^{-1}$ and $g_3 = g$ gives

$$d(g, g^{-1}) d(e_G, g) = g(d(g^{-1}, g)) d(g, e_G)$$

by [*1]

$$d(g, g^{-1}) d(e_G, e_G) = g(d(g^{-1}, g)) d(g, e_G)$$

by [*2]

$$d(g, g^{-1}) d(e_G, e_G) = g(d(g^{-1}, g)) g(d(e_G, e_G)),$$

i.e.

$$d(g, g^{-1})d(e_G, e_G) = g(d(g^{-1}, g)d(e_G, e_G)) \quad [*3]$$

Acting by g^{-1} on both sides gives:

$$g^{-1}(d(g, g^{-1})d(e_G, e_G)) = d(g^{-1}, g)d(e_G, e_G) \quad [*3']$$

Taking inverse of both sides gives:

$$g^{-1}(d(e_G, e_G)^{-1}d(g, g^{-1})^{-1}) = d(e_G, e_G)^{-1}d(g^{-1}, g)^{-1}$$

If we utilize this above we get:

$$a_2 = g_1^{-1}(a_1^{-1})d(e_G, e_G)^{-1}d(g_1^{-1}, g_1)^{-1} \quad \text{and} \quad g_2 = g_1^{-1}$$

This coincides with the other result.

Below it is verified that the inverse we solved for above is indeed a left and right inverse.

$$\begin{aligned} & (d_{e_G, e_G}^{-1}d_{g^{-1}, g}^{-1}g^{-1}(a^{-1}), g^{-1})(a, g) \\ &= (d_{e_G, e_G}^{-1}d_{g^{-1}, g}^{-1}g^{-1}(a^{-1})g^{-1}(a)d_{g^{-1}, g}, e_G) \\ &= (d_{e_G, e_G}^{-1}d_{g^{-1}, g}^{-1}d_{g^{-1}, g}, e_G) \\ &= (d_{e_G, e_G}^{-1}, e_G) \end{aligned}$$

$$\begin{aligned}
& (a, g)(d_{e_G, e_G}^{-1} d_{g^{-1}, g}^{-1} g^{-1}(a^{-1}), g^{-1}) \\
&= (a, g)((d_{g^{-1}, g} d_{e_G, e_G})^{-1} g^{-1}(a^{-1}), g^{-1}) \\
&= (ag((d_{g^{-1}, g} d_{e_G, e_G})^{-1} g^{-1}(a^{-1})), d_{g, g^{-1}}, e_G) \\
&= (ag((d_{g^{-1}, g} d_{e_G, e_G})^{-1}) g(g^{-1}(a^{-1})), d_{g, g^{-1}}, e_G) \\
&= (ag((d_{g^{-1}, g} d_{e_G, e_G})^{-1}) a^{-1} d_{g, g^{-1}}, e_G) \\
&= (aa^{-1} g((d_{g^{-1}, g} d_{e_G, e_G})^{-1}) d_{g, g^{-1}}, e_G) \quad A \text{ is abelian.} \\
&= (g((d_{g^{-1}, g} d_{e_G, e_G})^{-1}) d_{g, g^{-1}}, e_G) \\
&= ((d_{g, g^{-1}} d_{e_G, e_G})^{-1} d_{g, g^{-1}}, e_G) \quad \text{by } [*3] \\
&= (d_{e_G, e_G}^{-1} d_{g, g^{-1}}^{-1} d_{g, g^{-1}}, e_G) \\
&= (d_{e_G, e_G}^{-1}, e_G)
\end{aligned}$$

The homomorphisms, and exactness

2. $\pi((a, g)) = g$ is a group homomorphism, as

$$\pi((a_1, g_1)(a_2, g_2)) = \pi((a_1 g_1(a_2) d_{g_1, g_2}, g_1 g_2)) = g_1 g_2 = \pi((a_1, g_1)) \pi((a_2, g_2)).$$

By construction, π is surjective.

1. ι must map A to kernel of π which is $\{(a, e_G) \mid a \in A\}$ Suppose $\iota(a) = (i(a), e_G)$ for some function $i : A \rightarrow A$.

Then we have

$$\begin{aligned}
 \iota(a)\iota(b) &= (i(a), e_G)(i(b), e_G) \\
 &= (i(a)e_G(i(b))d_{e_G, e_G}, e_G) \\
 &= (i(a)i(b)d_{e_G, e_G}, e_G)
 \end{aligned}$$

For ι to be a homomorphism, this must equal $\iota(ab) = (i(ab), e_G)$ i.e.

$$i(ab) = i(a)i(b)d_{e_G, e_G}$$

Multiplying by d_{e_G, e_G} on both sides, while utilizing that A is abelian gives:

$$i(ab)d_{e_G, e_G} = i(a)d_{e_G, e_G}i(b)d_{e_G, e_G}$$

Therefore the function $i'(x) = i(x)d_{e_G, e_G}$ is multiplicative (or an endomorphism of A .)

The simplest choice, which insures injectiveness even when A has torsion, and also insures that all elements in $\{(a, e_G) \mid a \in A\}$ are covered, is to choose $i'(x) = x$, i.e. $i(a) = ad_{e_G, e_G}^{-1}$

So let

$$\iota(a) = (ad_{e_G, e_G}^{-1}, e_G)$$

Then

$$\begin{aligned}
 \iota(a)\iota(b) &= (ad_{e_G, e_G}^{-1})(bd_{e_G, e_G}^{-1}) \\
 &= (ad_{e_G, e_G}^{-1}e_G(bd_{e_G, e_G}^{-1})d_{e_G, e_G}, e_G) \\
 &= (ad_{e_G, e_G}^{-1}bd_{e_G, e_G}^{-1}d_{e_G, e_G}, e_G) \\
 &= (ad_{e_G, e_G}^{-1}b, e_G) \\
 &= (abd_{e_G, e_G}^{-1}, e_G) \quad A \text{ is abelian.} \\
 &= \iota(ab)
 \end{aligned}$$

is a homomorphism, with image

$$\{(a, e_G) \mid a \in A\} = \ker \pi$$

since

$$\iota(ad_{e_G, e_G}) = (ad_{e_G, e_G}d_{e_G, e_G}^{-1}, e_G) = (a, e_G).$$

The operation on the set $\{(a, e_G) \mid a \in A\}$ is defined by

$$(a_1, e_G)(a_2, e_G) = \iota(a_1d_{e_G, e_G})\iota(a_2d_{e_G, e_G}) = \iota(a_1a_2d_{e_G, e_G}^2) = (a_1a_2d_{e_G, e_G}, e_G)$$

Section

Let $s : G \rightarrow E$ be defined by $s(g) = (e_A, g)$, clearly we have $\pi(s(g)) = g$. On the other

hand,

$$\begin{aligned}
s(g)s(h)s(gh)^{-1} &= (e_A, g)(e_A, h)(e_A, gh)^{-1} \\
&= (e_A g(e_A) d_{g,h}, gh)(d_{e_G, e_G}^{-1} d_{(gh)^{-1}, gh}^{-1} (gh)^{-1} (e_A), (gh)^{-1}) \\
&= (d_{g,h}, gh)(d_{e_G, e_G}^{-1} d_{(gh)^{-1}, gh}^{-1}, (gh)^{-1}) \\
&= (d_{g,h} gh(d_{e_G, e_G}^{-1} d_{(gh)^{-1}, gh}^{-1}) d_{gh, (gh)^{-1}}, gh(gh)^{-1}) \\
&= (d_{g,h}(gh(d_{(gh)^{-1}, gh} d_{e_G, e_G})))^{-1} d_{gh, (gh)^{-1}}, e_G) \\
&= (d_{g,h}(d_{gh, (gh)^{-1}} d_{e_G, e_G}))^{-1} d_{gh, (gh)^{-1}}, e_G) \quad \text{by [*3]} \\
&= (d_{g,h}(d_{e_G, e_G}^{-1} d_{gh, (gh)^{-1}}^{-1}) d_{gh, (gh)^{-1}}, e_G) \\
&= (d_{g,h} d_{e_G, e_G}^{-1}, e_G) \\
&= \iota(d_{g,h})
\end{aligned}$$

$$s(g)s(h)s(gh)^{-1} = \iota(d_{g,h})$$

In particular:

$$\iota(d_{e_G, e_G}) = s(e_G)s(e_G)s(e_G)^{-1} = s(e_G)$$

Remark How would other sections compare? This can be understood by a previous lemma.

Inner Conjugation's compatibility with Group Action

Define $\mathcal{A} : G \times A \rightarrow E$ by

$$\mathcal{A}(g, x) = s(g)\iota(x)s(g)^{-1}$$

First note that

$$\pi(s(g)\iota(x)s(g)^{-1}) = \pi(s(g))\pi(\iota(x))\pi(s(g))^{-1} = ge_Gg^{-1} = e_G$$

using that π is a homomorphism. Hence image of $\mathcal{A}$ actually lies in $\ker \pi = \iota(A)$.

Now note:

$$\begin{aligned} \mathcal{A}(g, x) &= s(g)\iota(x)s(g)^{-1} \\ &= (e_A, g)(xd_{e_G, e_G}, e_G)(e_A, g)^{-1} \\ &= (e_Ag(xd_{e_G, e_G}^{-1})d_{g, e_G}, ge_G)(d_{e_G, e_G}^{-1}d_{g^{-1}, g}^{-1}, g^{-1}) \\ &= (g(xd_{e_G, e_G}^{-1})d_{g, e_G}, g)((d_{g^{-1}, g}d_{e_G, e_G})^{-1}, g^{-1}) \\ &= (g(x)g(d_{e_G, e_G}^{-1})g(d_{e_G, e_G}), g)((d_{g^{-1}, g}d_{e_G, e_G})^{-1}, g^{-1}) \quad \text{by [*2]} \\ &= (g(x), g)((d_{g^{-1}, g}d_{e_G, e_G})^{-1}, g^{-1}) \\ &= (g(x)g((d_{g^{-1}, g}d_{e_G, e_G})^{-1})d_{g, g^{-1}}, gg^{-1}) \\ &= (g(x)(d_{g, g^{-1}}d_{e_G, e_G})^{-1}d_{g, g^{-1}}, gg^{-1}) \quad \text{by [*3]} \\ &= (g(x)d_{e_G, e_G}^{-1}d_{g, g^{-1}}^{-1}d_{g, g^{-1}}, e_G) \\ &= (g(x)d_{e_G, e_G}^{-1}, e_G) \\ &= \iota(g(x)) \end{aligned}$$

Therefore we have

$$\mathcal{A}(g, x) = s(g)\iota(x)s(g)^{-1} = \iota(g(x))$$

Other relevant computations

$$\begin{aligned}
 \iota(a^{-1})(a, g) &= (a^{-1}d_{e_G, e_G}^{-1}, e_G)(a, g) \\
 &= (a^{-1}d_{e_G, e_G}^{-1}e_G(a)d_{e_G, g}, e_Gg) \\
 &= (a^{-1}d_{e_G, e_G}^{-1}ad_{e_G, g}, g) \\
 &= (a^{-1}ad_{e_G, e_G}^{-1}d_{e_G, g}, g) \quad A \text{ is abelian} \\
 &= (d_{e_G, e_G}^{-1}d_{e_G, e_G}, g) \\
 &= (e_A, g) \quad \text{by } [*1] \\
 &= s(g)
 \end{aligned}$$

Therefore we have

$$(a, g) = \iota(a)s(g)$$

Since $(a, g) = \iota(a)s(g)$ we have

$$\begin{aligned}
 \iota(a)s(g) &= s(g)s(g)^{-1}\iota(a)s(g) = s(g)\iota(g^{-1}(a)) = s(g)\iota(g^{-1}(a))\iota(a^{-1})\iota(a) \\
 &= s(g)\iota(g^{-1}(a)a^{-1})\iota(a)
 \end{aligned}$$

or

$$\iota(a)s(g) = \iota(a)s(g)\iota(a^{-1})\iota(a).$$

$$\begin{aligned}
\iota(a)s(g)\iota(a^{-1}) &= (ad_{e_G, e_G}^{-1}, e_G)(e_A, g)(a^{-1}d_{e_G, e_G}^{-1}, e_G) \\
&= (ad_{e_G, e_G}^{-1}d_{e_G, g}, g)(a^{-1}d_{e_G, e_G}^{-1}, e_G) \\
&= (ad_{e_G, e_G}^{-1}d_{e_G, g}g(a^{-1}d_{e_G, e_G}^{-1})d_{g, e_G}, g) \\
&= (ad_{e_G, e_G}^{-1}d_{e_G, g}g(a^{-1})g(d_{e_G, e_G}^{-1})g(d_{e_G, e_G}), g) \quad \text{by [*2]} \\
&= (ad_{e_G, e_G}^{-1}d_{e_G, e_G}g(a^{-1}), g) \quad \text{by [*1]} \\
&= (ag(a^{-1}), g)
\end{aligned}$$

$$\begin{aligned}
s(g)\iota(g^{-1}(a)a^{-1}) &= (e_A, g)(g^{-1}(a)a^{-1}d_{e_G, e_G}^{-1}, e_G) \\
&= (g(g^{-1}(a)a^{-1}d_{e_G, e_G}^{-1})d_{g, e_G}, g) \\
&= (ag(a^{-1})g(d_{e_G, e_G}^{-1})d_{g, e_G}, g) \\
&= (ag(a^{-1})g(d_{e_G, e_G}^{-1})g(d_{e_G, e_G}), g) \quad \text{by [*2]} \\
&= (ag(a^{-1}), g)
\end{aligned}$$

Therefore we have

$$(a, g) = (s(g)\iota(g^{-1}(a)a^{-1}))\iota(a) = (\iota(a)s(g)\iota(a^{-1}))\iota(a) = (ag(a^{-1}), g)(ad_{e_G, e_G}^{-1}, e_G)$$

Summary of Results

The equation satisfied by $d : G \times G \rightarrow A$ is

$$\tau_1(d_{\tau_2, \tau_3})d_{\tau_1, \tau_2 \tau_3} = d_{\tau_1, \tau_2}d_{\tau_1 \tau_2, \tau_3}$$

$E = A \times G$ as a set. Group operation is given by:

$$(a_1, g_1)(a_2, g_2) = (a_1 g_1(a_2) d_{g_1, g_2}, g_1 g_2)$$

The unit element is given by

$$(d_{e_G, e_G}^{-1}, e_G)$$

The inverse is given by

$$(a, g)^{-1} = (d_{e_G, e_G}^{-1} d_{g^{-1}, g}^{-1} g^{-1}(a^{-1}), g^{-1}) = ((d_{g^{-1}, g} d_{e_G, e_G})^{-1} g^{-1}(a^{-1}), g^{-1})$$

The homomorphisms ι and π are given by:

$$\iota(a) = (a d_{e_G, e_G}^{-1}, e_G)$$

$$\pi((a, g)) = g$$

The section is given by:

$$s(g) = (e_A, g)$$

It satisfies:

$$s(g)s(h)s(gh)^{-1} = \iota(d_{g, h})$$

Group action of G on A coincides with inner conjugation in E :

$$\mathcal{A}(g, x) = s(g)\iota(x)s(g)^{-1} = \iota(g(x))$$

One can derive the following equalities from the constraint satisfied by d , by special choices for τ_1, τ_2, τ_3 :

$$d(e_G, e_G) = d(e_G, g) \quad [*1]$$

$$d(g, e_G) = g(d(e_G, e_G)) \quad [*2]$$

$$d(g, g^{-1})d(e_G, e_G) = g(d(g^{-1}, g)d(e_G, e_G)) \quad [*3]$$

Furthermore the following also holds:

$$(a, g) = \iota(a)s(g)$$

and

$$(a, g) = (s(g)\iota(g^{-1}(a)a^{-1}))\iota(a) = (\iota(a)s(g)\iota(a^{-1}))\iota(a) = (ag(a^{-1}), g)(ad_{e_G, e_G}^{-1}, e_G)$$

Also

$$\iota(d_{e_G, e_G}) = s(e_G)$$

Questions How much of the abelianness of A can be dropped? What is inner conjugation in E more generally?

Inner Conjugation in E

$$\begin{aligned} & (a_1, g_1)(a_2, g_2)(a_1, g_1)^{-1} \\ &= \iota(a_1)s(g_1)\iota(a_2)s(g_2)(\iota(a_1)s(g_1))^{-1} \\ &= \iota(a_1)s(g_1)\iota(a_2)s(g_2)s(g_1)^{-1}\iota(a_1^{-1}) \\ &= \iota(a_1)s(g_1)\iota(a_2)s(g_1)^{-1}s(g_1)s(g_2)s(g_1)^{-1}\iota(a_1^{-1})s(g_1)s(g_2)^{-1}s(g_1)^{-1}s(g_1)s(g_2)s(g_1)^{-1} \\ &= \iota(a_1)\iota(g_1(a_2))\iota(g_1(g_2(g_1^{-1}(a_1^{-1}))))s(g_1)s(g_2)s(g_1g_2)^{-1}s(g_1g_2) \\ & \quad s(g_1^{-1})s(g_1g_2g_1^{-1})^{-1}s(g_1g_2g_1^{-1})s(g_1^{-1})^{-1}s(g_1)^{-1} \\ &= \iota(a_1g_1(a_2)(g_1g_2g_1^{-1})(a_1^{-1})d_{g_1, g_2}d_{g_1g_2, g_1^{-1}})s(g_1g_2g_1^{-1})(s(g_1)s(g_1^{-1}))^{-1} \end{aligned}$$

$$\begin{aligned}
&= \iota(a_1 g_1(a_2)(g_1 g_2 g_1^{-1})(a_1^{-1})d_{g_1, g_2}d_{g_1 g_2, g_1^{-1}})s(g_1 g_2 g_1^{-1})(s(g_1)s(g_1^{-1})s(e_G)^{-1}s(e_G))^{-1} \\
&= \iota(a_1 g_1(a_2)(g_1 g_2 g_1^{-1})(a_1^{-1})d_{g_1, g_2}d_{g_1 g_2, g_1^{-1}})s(g_1 g_2 g_1^{-1})(d_{g_1, g_1^{-1}}s(e_G))^{-1} \\
&= \iota(a_1 g_1(a_2)(g_1 g_2 g_1^{-1})(a_1^{-1})d_{g_1, g_2}d_{g_1 g_2, g_1^{-1}})s(g_1 g_2 g_1^{-1})s(e_G)^{-1}d_{g_1, g_1^{-1}}^{-1} \\
&= \iota(a_1 g_1(a_2)(g_1 g_2 g_1^{-1})(a_1^{-1})d_{g_1, g_2}d_{g_1 g_2, g_1^{-1}})s(g_1 g_2 g_1^{-1})(d_{e_G, e_G})^{-1}d_{g_1, g_1^{-1}}^{-1} \\
&= \iota(a_1 g_1(a_2)(g_1 g_2 g_1^{-1})(a_1^{-1})d_{g_1, g_2}d_{g_1 g_2, g_1^{-1}})s(g_1 g_2 g_1^{-1})(d_{e_G, e_G})^{-1}d_{g_1, g_1^{-1}}^{-1}s(g_1 g_2 g_1^{-1})^{-1} \\
&\quad s(g_1 g_2 g_1^{-1}) \\
&= \iota(a_1 g_1(a_2)(g_1 g_2 g_1^{-1})(a_1^{-1})d_{g_1, g_2}d_{g_1 g_2, g_1^{-1}}(g_1 g_2 g_1^{-1})((d_{e_G, e_G})^{-1}d_{g_1, g_1^{-1}}^{-1}))s(g_1 g_2 g_1^{-1}) \\
&= (a_1 g_1(a_2)d_{g_1, g_2}d_{g_1 g_2, g_1^{-1}}(g_1 g_2 g_1^{-1})(a_1^{-1}(d_{e_G, e_G})^{-1}d_{g_1, g_1^{-1}}^{-1}), g_1 g_2 g_1^{-1})
\end{aligned}$$

Let $x^g = gxg^{-1}$

$$\begin{aligned}
&(a_1, g_1)(a_2, g_2)(a_1, g_1)^{-1} \\
&= (a_1 g_1(a_2)d_{g_1, g_2}, g_1 g_2)((d_{g_1^{-1}, g_1}d_{e_G, e_G})^{-1}g_1^{-1}(a_1^{-1}), g_1^{-1}) \\
&= (a_1 g_1(a_2)d_{g_1, g_2}(g_1 g_2)((d_{g_1^{-1}, g_1}d_{e_G, e_G})^{-1}g_1^{-1}(a_1^{-1}))d_{g_1 g_2, g_1^{-1}}, g_1 g_2 g_1^{-1}) \\
&= (a_1 g_1(a_2)d_{g_1, g_2}(g_1 g_2 g_1^{-1})(g_1((d_{g_1^{-1}, g_1}d_{e_G, e_G})^{-1})a_1^{-1})d_{g_1 g_2, g_1^{-1}}, g_1 g_2 g_1^{-1})
\end{aligned}$$

$$\begin{aligned}
&= (a_1 g_1(a_2) d_{g_1, g_2}(g_2^{g_1})(g_1((d_{g_1^{-1}, g_1} d_{e_G, e_G})^{-1}) a_1^{-1}) d_{g_1 g_2, g_1^{-1}}, g_2^{g_1}) \\
&= (a_1 g_1(a_2) d_{g_1, g_2}(g_2^{g_1})((d_{g_1, g_1^{-1}} d_{e_G, e_G})^{-1} a_1^{-1}) d_{g_1 g_2, g_1^{-1}}, g_2^{g_1}) \text{ by } [*3] \\
&= (a_1 g_1(a_2) d_{g_1, g_2}(g_2^{g_1})((d_{g_1, g_1^{-1}} d_{e_G, e_G})^{-1})(g_2^{g_1})(a_1^{-1}) d_{g_1 g_2, g_1^{-1}}, g_2^{g_1}) \\
&= (a_1 g_1(a_2)(g_2^{g_1})(a_1^{-1}) d_{g_1, g_2} d_{g_1 g_2, g_1^{-1}}(g_2^{g_1})((d_{g_1, g_1^{-1}} d_{e_G, e_G})^{-1}), g_2^{g_1}) \quad A \text{ is abelian.}
\end{aligned}$$

Note

$$d_{g_1, g_2} d_{g_1 g_2, g_1^{-1}} = g_1(d_{g_2, g_1^{-1}}) d_{g_1, g_2 g_1^{-1}}$$

which may be replaced above.

If $g_2 = e_G$, then above reduces to:

$$\begin{aligned}
(a_1, g_1) \iota(a_2 d_{e_G, e_G})(a_1, g_1)^{-1} &= (g_1(a_2 d_{e_G, e_G})(d_{e_G, e_G})^{-1}, e_G) \\
&= \iota(g_1(a_2 d_{e_G, e_G}))
\end{aligned}$$

which coincides with the earlier computation.

Question Is $t : E \rightarrow A$ defined by $t((a, g)) = a$ a group homomorphism? Note

$$t((a_1, g_1)(a_2, g_2)) = t((a_1 g_1(a_2) d_{g_1, g_2}, g_1 g_2)) = a_1 g_1(a_2) d_{g_1, g_2}$$

but

$$t((a_1, g_1)) t((a_2, g_2)) = a_1 a_2.$$

This will be a group homomorphism if

$$a_2^{-1} g_1(a_2) = d_{g_1, g_2}$$

but note that left hand-side is independent of g_2 .

Also note that if there is a group homomorphism, then $t \circ \iota$ is an endomorphism of A and

$\iota \circ t$ is an endomorphism of E .

Lemma 106 (*Extension isomorphism*) Let A be an abelian group and G a group acting on A . Suppose we are given $d^i : G \times G \rightarrow A$ satisfying

$$\tau_1(d_{\tau_2, \tau_3})d_{\tau_1, \tau_2 \tau_3} = d_{\tau_1, \tau_2}d_{\tau_1 \tau_2, \tau_3}$$

for $d = d^i$ with $i = 1, 2$. Let E_i be the corresponding extension groups. Then $E_1 \cong E_2$ and the extensions are extension-isomorphic, meaning that the diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & A & \xrightarrow{\iota_1} & E_1 & \xrightarrow{\pi_1} & G \longrightarrow 1 \\ & & \downarrow \text{id} & & \downarrow \varphi & & \downarrow \text{id} \\ 1 & \longrightarrow & A & \xrightarrow{\iota_2} & E_2 & \xrightarrow{\pi_2} & G \longrightarrow 1 \end{array}$$

is commutative, if and only if there exists a function $f : G \rightarrow A$ such that

$$d^1(g, h)(d^2(g, h))^{-1} = f(g)\mathcal{A}(g, f(h))f(gh)^{-1}$$

Remark

The lemma can be interpreted to say that extension isomorphisms are in one-to-one correspondence with functions f satisfying the stated equality.

In fact the correspondence is given by

$$\iota_2(f(x)) = \varphi(s_1(x))s_2(x)^{-1}$$

equivalent to

$$\iota_1(f(x)) = s_1(x)\varphi^{-1}(s_2(x)^{-1})$$

as shown in the proof below.

Homomorphism is an isomorphism

If $\varphi : E_1 \rightarrow E_2$ is a homomorphism such that the diagram is commutative, then

Suppose $x \in \ker \varphi$. Then $\pi_1(x) = \pi_2(\varphi(x)) = \pi_2(e_{E_2}) = e_G$, so that $x \in \ker \pi_1 = \text{im } \iota_1$.

Then there exists $a \in A$ such that $\iota_1(a) = x$. Since $\iota_2(a) = \varphi(\iota_1(a)) = \varphi(x) = e_{E_2}$, and ι_2 is injective, $a = e_A$, so that $x = \iota_1(a) = \iota_1(e_A) = e_A$. Hence φ is injective.

Let $y \in E_2$. Choose $x \in E_1$, such that $\pi_1(x) = \pi_2(y)$. (Say $x = s_1(\pi_2(y))$.) Then $\pi_2(\varphi(x)) = \pi_1(x) = \pi_2(y)$, so that $y\varphi(x)^{-1} \in \ker \pi_2 = \text{im } \iota_2$. Then there exists $a \in A$, such that $\iota_2(a) = y\varphi(x)^{-1}$. Hence $y = \iota_2(a)\varphi(x) = \varphi(\iota_1(a))\varphi(x) = \varphi(\iota_1(a)x)$. Hence φ is surjective.

Note $a = \iota_2^{-1}(y\varphi(s_1(\pi_2(y)))^{-1})$, and $x = s_1(\pi_2(y))$.

If there is an isomorphism, then the required function exists

Suppose $\varphi : E_1 \rightarrow E_2$ is an isomorphism.

Since $g = \pi_1(a, g) = \pi_2(\varphi(a, g))$ we have that

$$\varphi((a, g)) = (\tilde{\varphi}(a, g), g)$$

for some function $\tilde{\varphi} : A \times G \rightarrow A$. In fact $\tilde{\varphi}$ is projection on first coordinate of φ , but projection is not necessarily a group homomorphism.

On the other hand we have

$$\varphi((a, g)) = \varphi(\iota_1(a)s_1(g)) = \varphi(\iota_1(a))\varphi(s_1(g)) = \iota_2(a)\varphi(s_1(g))$$

Since

$$\pi_2(\varphi(s_1(g))) = \pi_1(s_1(g)) = g = \pi_2(s_2(g))$$

$\varphi(s_1(g))$ is another section for $\pi_2 : E_2 \rightarrow G$. But by previous lemma, different sections of the same extension are related by:

$$d^2(g, h) = f(g)\mathcal{A}(g, f(h))f(gh)^{-1}d^1(g, h)$$

for $f(g) = f^2(g) = a^2(g)a^1(g)^{-1}$ where d^2 is the function associated with a^2 and d^1 that associated with a^1 .

Above, write $\varphi(d_{g,h}^1)$ for $d^2(g, h)$ and $d_{g,h}^2$ for $d^1(g, h)$ and $f(g) = f^2(g) = \varphi(s_1(g))s_2(g)^{-1}$. (i.e. $a^2(g) = \varphi(s_1(g))$ and $a^1(g) = s_2(g)$). Then the equation is:

$$\varphi(\iota_1(d^1(g, h))) = f(g)\mathcal{A}(g, f(h))f(gh)^{-1}\iota_2(d^2(g, h))$$

where $f(g) = \varphi(s_1(g))s_2(g)^{-1}$.

Note $\pi_2(f(g)) = \pi_2(\varphi(s_1(g))s_2(g)^{-1}) = \pi_2(\varphi(s_1(g)))\pi_2(s_2(g))^{-1} = \pi_1(s_1(g))g^{-1} = gg^{-1} = e_G$. Hence $f(g) \in \ker \pi_2 = \text{im } \iota_2$. Define $f(g)$ as $\iota_2^{-1}(f(g))$.

Rewriting the above gives:

$$d^1(g, h)(d^2(g, h))^{-1} = f(g)\mathcal{A}(g, f(h))f(gh)^{-1}$$

Existence of such a function implies existence of a homomorphism

Given $f : G \rightarrow A$ satisfying the stated identity,

define:

$$\varphi(s_1(g)) = \iota_2(f(g))s_2(g),$$

and

$$\varphi(\iota_1(a)) = \iota_2(a).$$

So that

$$\varphi(\iota_1(a)s_1(g)) = \iota_2(af(g))s_2(g).$$

This defines a homomorphism: Since

$$(a_1, g_1)(a_2, g_2) = (a_1g_1(a_2)d^1(g_1, g_2), g_1g_2)$$

in E_1 . And

$$\varphi((a_i, g_i)) = (a_if(g_i), g_i)$$

for $i = 1, 2$. and

$$\varphi(((a_1g_1(a_2)d^1(g_1, g_2), g_1g_2))) = (a_1g_1(a_2)d^1(g_1, g_2)f(g_1g_2), g_1g_2)$$

and

$$(a_1f(g_1), g_1)(a_2f(g_2), g_2) = (a_1f(g_1)g_1(a_2f(g_2))d^2(g_1, g_2), g_1g_2)$$

in E_2 . But

$$\begin{aligned} & t(\varphi((a_1, g_1))\varphi((a_2, g_2))) \\ &= a_1f(g_1)g_1(a_2f(g_2))d^2(g_1, g_2) \\ &= a_1f(g_1)g_1(a_2)g_1(f(g_2))d^2(g_1, g_2) \\ &= a_1g_1(a_2)f(g_1)g_1(f(g_2))d^2(g_1, g_2) \quad A \text{ is abelian.} \\ &= a_1g_1(a_2)d^1(g_1, g_2)f(g_1g_2) \quad \text{Equation satisfied by } f \\ &= t(\varphi((a_1, g_1)(a_2, g_2))) \end{aligned}$$

Where $t : E_2 \rightarrow A$, is projection on the first coordinate. The second coordinates also match.

On the other hand, φ forms a commutative diagram by construction.

Restriction of homomorphism on A

Since $\varphi(\iota_1(a)) = \iota_2(a)$ so that

$$\tilde{\varphi}(a(d_{e_G, e_G}^1)^{-1}, e_G) = a(d_{e_G, e_G}^2)^{-1}$$

Writing ad_{e_G, e_G}^1 instead of a above we get

$$\tilde{\varphi}(a, e_G) = ad^1(e_G, e_G)(d_{e_G, e_G}^2)^{-1}$$

Expression for f

Note

$$\begin{aligned}
 f(g) &= \varphi(s_1(g))s_2(g)^{-1} \\
 &= \varphi((e_A, g))(e_A, g)^{-1} \\
 &= (\tilde{\varphi}((e_A, g)), g)((d_{g^{-1}, g}^2 d_{e_G, e_G}^2)^{-1}, g^{-1}) \\
 &= (\tilde{\varphi}((e_A, g))g((d_{g^{-1}, g}^2 d_{e_G, e_G}^2)^{-1})d_{g, g^{-1}}^2, e_G) \\
 &= (\tilde{\varphi}((e_A, g))(d_{g, g^{-1}}^2 d_{e_G, e_G}^2)^{-1}d_{g, g^{-1}}^2, e_G) \\
 &= (\tilde{\varphi}((e_A, g))(d_{e_G, e_G}^2)^{-1}(d_{g, g^{-1}}^2)^{-1}d_{g, g^{-1}}^2, e_G) \\
 &= (\tilde{\varphi}((e_A, g))(d_{e_G, e_G}^2)^{-1}, e_G) \\
 &= \iota_2(\tilde{\varphi}((e_A, g)))
 \end{aligned}$$

Redundant Check $\iota_2(f(g)) = \varphi(s_1(g))s_2(g)^{-1}$ being the defining equation for f , f satisfies the mentioned equation:

$$d^1(g, h)(d^2(g, h))^{-1} = f(g)\mathcal{A}(g, f(h))f(gh)^{-1}$$

$$\begin{aligned}
& f(g)\mathcal{A}(g, f(h))f(gh)^{-1} \\
&= \varphi(s_1(g))s_2(g)^{-1}\mathcal{A}(g, \varphi(s_1(h))s_2(h)^{-1})(\varphi(s_1(gh))s_2(gh)^{-1})^{-1} \\
&= \varphi(s_1(g))s_2(g)^{-1}s_2(g)\varphi(s_1(h))s_2(h)^{-1}s_2(g)^{-1}(\varphi(s_1(gh))s_2(gh)^{-1})^{-1} \\
&= \varphi(s_1(g))\varphi(s_1(h))\varphi(s_1(gh)^{-1})\varphi(s_1(gh))s_2(h)^{-1}s_2(g)^{-1}(\varphi(s_1(gh))s_2(gh)^{-1})^{-1} \\
&= \varphi(s_1(g)s_1(h)(s_1(gh))^{-1})\varphi(s_1(gh))s_2(h)^{-1}s_2(g)^{-1}s_2(gh)\varphi(s_1(gh))^{-1} \\
&= \varphi(s_1(g)s_1(h)(s_1(gh))^{-1})\varphi(s_1(gh))s_2(gh)^{-1}s_2(gh)s_2(h)^{-1}s_2(g)^{-1}s_2(gh)\varphi(s_1(gh))^{-1} \\
&= \varphi(d^1(g, h))\varphi(s_1(gh))s_2(gh)^{-1}(d^2(g, h))^{-1}s_2(gh)\varphi(s_1(gh))^{-1} \\
&= \varphi(d^1(g, h))\mathcal{A}(gh, \mathcal{A}((gh)^{-1}, (d^2(g, h))^{-1})) \\
&= \varphi(d^1(g, h))(d^2(g, h))^{-1}
\end{aligned}$$

But here note that $d^1(g, h)$ is really $\iota_1(d^1(g, h))$ and $d^2(g, h) = \iota_2(d^2(g, h))$. so that the above equals

$$\varphi(\iota_1(d^1(g, h)))\iota_2((d^2(g, h))^{-1}) = \iota_2(d^1(g, h)(d^2(g, h))^{-1})$$

reproving the formula. Note that since $\varphi(s_1(g))$ and $s_2(g)$ are two different sections of the same map, the action they generate on A is identical.

Summary of Results

$$f(g) = \varphi(s_1(g))s_2(g)^{-1}$$

Lemma 107 (*Extension Isomorphisms 2 – composition*) If $\rho : E_2 \rightarrow E_3$ and $\sigma : E_1 \rightarrow E_2$,

are two extension isomorphisms, then we have the equality

$$f_{\rho\sigma} = \rho(f_\sigma)f_\rho$$

where

$$f_\mu(g) = \mu(s_i(g))(s_t(g))^{-1}$$

and $\mu : E_i \rightarrow E_t$ is an extension isomorphism, and s_i is section of $\pi : E_i \rightarrow G$, and s_t is section of $\pi : E_t \rightarrow G$.

$$\begin{aligned} \rho(f_\sigma(g))f_\rho(g) &= \rho(\sigma(s_1(g))(s_2(g))^{-1})\rho(s_2(g))(s_3(g))^{-1} \\ &= \rho(\sigma(s_1(g))(s_2(g))^{-1}s_2(g))(s_3(g))^{-1} \\ &= \rho(\sigma(s_1(g)))(s_3(g))^{-1} \\ &= (\rho \circ \sigma)(s_1(g))(s_3(g))^{-1} \\ &= f_{\rho\sigma}(g) \end{aligned}$$

Lemma 108 (*Split extensions*) An extension $1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1$ with a section of $\pi : E \rightarrow G$, called $a : G \rightarrow E$, splits (meaning there exists a section that is a homomorphism), if and only if there exists a function $b : G \rightarrow A$, that satisfies

$$b(\tau_1)\tau_1(b(\tau_2))d_{\tau_1, \tau_2} = b(\tau_1\tau_2)$$

with $\iota(b(\tau))a(\tau)$ being the homomorphism section.

Since $\pi(\iota(b(\tau))a(\tau)) = \pi(\iota(b(\tau)))\pi(a(\tau)) = \tau$, hence $\iota(b(\tau))a(\tau)$ is indeed a section. On the other hand,

Starting with the given equation:

$$b(\tau_1)\tau_1(b(\tau_2))d_{\tau_1,\tau_2} = b(\tau_1\tau_2)$$

$$b(\tau_1)\tau_1(b(\tau_2))d_{\tau_1,\tau_2}a(\tau_1\tau_2) = b(\tau_1\tau_2)a(\tau_1\tau_2)$$

$$b(\tau_1)a(\tau_1)b(\tau_2)a(\tau_1)^{-1}a(\tau_1)a(\tau_2) = b(\tau_1\tau_2)a(\tau_1\tau_2)$$

$$b(\tau_1)a(\tau_1)b(\tau_2)a(\tau_2) = b(\tau_1\tau_2)a(\tau_1\tau_2)$$

This proves that $b(\tau)a(\tau)$ is a homomorphism.

Above $b(\tau)$ really means $\iota(b(\tau))$ and $\tau(b(\tau'))$ really means $\iota(\tau(b(\tau')))) = a(\tau)\iota(b(\tau'))a(\tau)^{-1}$.

On the other hand, if the sequence splits and $s : G \rightarrow E$ is a homomorphic section, then define $b(\tau) = s(\tau)a(\tau)^{-1}$. And note that

$$\begin{aligned} & b(\tau_1)\tau_1(b(\tau_2))d_{\tau_1,\tau_2} \\ &= s(\tau_1)a(\tau_1)^{-1}a(\tau_1)s(\tau_2)a(\tau_2)^{-1}a(\tau_1)^{-1}a(\tau_1)a(\tau_2)a(\tau_1\tau_2)^{-1} \\ &= s(\tau_1)s(\tau_2)a(\tau_1\tau_2)^{-1} \\ &= s(\tau_1\tau_2)a(\tau_1\tau_2)^{-1} \\ &= b(\tau_1)b(\tau_2) \end{aligned}$$

Therefore b satisfies the stated equation.

8.10.3. Further Discussion

We are going to discuss results related to the following question: Can extension isomorphisms be identified with elements in G ? Directly we can not reach a definite conclusion, however the results outlined below list what can be concluded close to this question.

Lemma 109 (*Group action on Extension 1*) *Suppose G acts on E that restricts to the previous action (of inner conjugation) on A . Furthermore suppose, $\pi(g(x)) = \pi(x)$, for $x \in E$. Then each $g \in Z(G)$ determines an extension isomorphism.*

By previous lemma 106, extension isomorphism lemma, it suffices to prove existence of a function $f : G \rightarrow A$, satisfying

$$d_{g,h}^1(d_{g,h}^2)^{-1} = f(g)\mathcal{A}(g, f(h))f(gh)^{-1}$$

For the function, choose $\iota(f_g(x)) = g(s(x))s(x)^{-1}$. Note that $\pi(g(s(x))) = \pi(s(x))$, by assumption, so that right-hand side lies in $\iota(A)$.

On the other hand,

$$\begin{aligned}
& f(x)\mathcal{A}(x, f(y))f(xy)^{-1} \\
&= f(x)s(x)f(y)s(x)^{-1}f(xy)^{-1} \\
&= f(x)s(x)f(y)s(y)s(y)^{-1}s(x)^{-1}f(xy)^{-1} \\
&= f(x)s(x)f(y)s(y)s(xy)^{-1}s(xy)s(y)^{-1}s(x)^{-1}f(xy)^{-1} \\
&= f(x)s(x)f(y)s(y)s(xy)^{-1}(s(x)s(y)s(xy)^{-1})^{-1}f(xy)^{-1} \\
&= f(x)s(x)f(y)s(y)s(xy)^{-1}d_{x,y}^{-1}f(xy)^{-1} \\
&= f(x)s(x)f(y)s(y)s(xy)^{-1}f(xy)^{-1}d_{x,y}^{-1} \quad A \text{ is abelian.} \\
&= f(x)s(x)f(y)s(y)(f(xy)s(xy))^{-1}d_{x,y}^{-1} \\
&= g(s(x))g(s(y))g(s(xy))^{-1}d_{x,y}^{-1} \\
&= g(s(x)s(y)s(xy)^{-1})d_{x,y}^{-1} \\
&= g(d_{x,y})d_{x,y}^{-1} \\
&= f_g(d_{x,y})
\end{aligned}$$

Writing $d_{x,y}^1 = g(d_{x,y})$ and $d_{x,y}^2 = d_{x,y}$, we see that this matches the required condition for f_g to define an extension isomorphism.

Of course it is necessary to check that $d_{x,y}^1 = g(d_{x,y})$ defines an extension.

On the other hand, if $g \in Z(G)$, then we have:

$$\tau(g(d_{x,y})) = g(\tau(d_{x,y})) = g(d_{\tau,x}d_{\tau x,y}d_{\tau,x,y}^{-1})$$

Hence in that case, $g(d_{x,y})$ defines an extension.

Remark

Note that it suffices to determine $g(s(x))s(x)^{-1} = f_g(x)$ for $x \in G$, to determine the action of G on E completely.

Lemma 110 *If $d^2(g, h) = f(g)\mathcal{A}(g, f(h))f(gh)^{-1}d_{g,h}$ for some function $f : G \rightarrow A$, and d satisfies the equation*

$$\tau(d_{x,y}) = d_{\tau,x}d_{\tau x,y}d_{\tau,xy}^{-1}$$

then d^2 satisfies the same equation.

Remark It may be that this lemma is redundant in view of lemma "Extension Isomorphism".

Let $u(g, h) = f(g)\mathcal{A}(g, f(h))f(gh)^{-1}$. The property follows if

$$\tau(u(x, y)) = u(\tau, x)u(\tau x, y)u(\tau, xy)^{-1}$$

$$\begin{aligned}
& u(\tau, x)u(\tau x, y)u(\tau, xy)^{-1} \\
&= u(\tau, x)u(\tau x, y) \left(f(\tau)\mathcal{A}(\tau, f(xy))f(\tau xy)^{-1} \right)^{-1} \\
&= u(\tau, x)u(\tau x, y) \left(f(\tau xy)\mathcal{A}(\tau, f(xy))^{-1}f(\tau)^{-1} \right) \\
&= \left(f(\tau)\mathcal{A}(\tau, f(x))f(\tau x)^{-1} \right) \left(f(\tau x)\mathcal{A}(\tau x, f(y))f(\tau xy)^{-1} \right) \left(f(\tau xy)\mathcal{A}(\tau, f(xy))^{-1}f(\tau)^{-1} \right) \\
&= f(\tau)\mathcal{A}(\tau, f(x))\mathcal{A}(\tau x, f(y))\mathcal{A}(\tau, f(xy))^{-1}f(\tau)^{-1} \\
&= f(\tau)f(\tau)^{-1}\mathcal{A}(\tau, f(x))\mathcal{A}(\tau x, f(y))\mathcal{A}(\tau, f(xy))^{-1} \\
&= \mathcal{A}(\tau, f(x))\mathcal{A}(\tau, \mathcal{A}(x, f(y)))\mathcal{A}(\tau, f(xy))^{-1} \\
&= \mathcal{A}(\tau, f(x))\mathcal{A}(x, f(y))f(xy)^{-1} \\
&= \mathcal{A}(\tau, u(x, y))
\end{aligned}$$

Lemma 111 (Group action on extension 2) *In light of the previous proposition, we can lift the assumption that $g \in Z(G)$, in the prior lemma.*

Question

Does the equation

$$\tau_1(d_{\tau_2, \tau_3})d_{\tau_1, \tau_2 \tau_3} = d_{\tau_1, \tau_2}d_{\tau_1 \tau_2, \tau_3}$$

define an action of G on A ? The answer is yes if it satisfies another simpler equation, and on the subgroup of A generated by the image of $d : G \times G \rightarrow A$.

Lemma 112 (Group action induced by d – incomplete) *Let $d : G \times G \rightarrow A$ be a function. The equation*

$$\mathcal{A}(\sigma, d_{\tau_1, \tau_2}) = d_{\sigma, \tau_1}d_{\sigma \tau_1, \tau_2}d_{\sigma, \tau_1 \tau_2}^{-1}$$

and the assumed equality

$$d_{e_G, e_G} = d_{e_G, \tau}$$

imply that $\mathcal{A} : G \times \langle \text{im } d \rangle \rightarrow \langle \text{im } d \rangle$ is a group action.

Note that the action is defined on the generators of a group, therefore defines a map $G \rightarrow \text{Aut}(\langle \text{im } d \rangle)$. To see that it is a group homomorphism, note

$$\begin{aligned}
 & \mathcal{A}(\mu, \mathcal{A}(\sigma, d_{\tau_1, \tau_2})) \\
 = & \mathcal{A}(\mu, d_{\sigma, \tau_1} d_{\sigma \tau_1, \tau_2} d_{\sigma, \tau_1 \tau_2}^{-1}) \\
 = & \mathcal{A}(\mu, d_{\sigma, \tau_1}) \mathcal{A}(\mu, d_{\sigma \tau_1, \tau_2}) \mathcal{A}(\mu, d_{\sigma, \tau_1 \tau_2})^{-1} \quad \text{using definition of action on generators.} \\
 = & d_{\mu, \sigma} d_{\mu \sigma, \tau_1} d_{\mu, \sigma \tau_1}^{-1} d_{\mu, \sigma \tau_1} d_{\mu \sigma \tau_1, \tau_2} d_{\mu, \sigma \tau_1 \tau_2}^{-1} (d_{\mu, \sigma} d_{\mu \sigma, \tau_1 \tau_2} d_{\mu, \sigma \tau_1 \tau_2}^{-1})^{-1} \\
 = & d_{\mu, \sigma} d_{\mu \sigma, \tau_1} d_{\mu, \sigma \tau_1}^{-1} d_{\mu, \sigma \tau_1} d_{\mu \sigma \tau_1, \tau_2} d_{\mu, \sigma \tau_1 \tau_2}^{-1} d_{\mu, \sigma \tau_1 \tau_2} d_{\mu \sigma, \tau_1 \tau_2}^{-1} d_{\mu, \sigma}^{-1} \\
 = & d_{\mu, \sigma} d_{\mu \sigma, \tau_1} d_{\mu \sigma \tau_1, \tau_2} d_{\mu \sigma, \tau_1 \tau_2}^{-1} d_{\mu, \sigma}^{-1} \\
 = & d_{\mu, \sigma} d_{\mu, \sigma}^{-1} d_{\mu \sigma, \tau_1} d_{\mu \sigma \tau_1, \tau_2} d_{\mu \sigma, \tau_1 \tau_2}^{-1} \quad A \text{ is abelian.} \\
 = & d_{\mu \sigma, \tau_1} d_{\mu \sigma \tau_1, \tau_2} d_{\mu \sigma, \tau_1 \tau_2}^{-1} \\
 = & \mathcal{A}(\mu \sigma, d_{\tau_1, \tau_2})
 \end{aligned}$$

On the other hand, note

$$\begin{aligned}
 & \mathcal{A}(e_G, d_{\tau_1, \tau_2}) \\
 &= d_{e_G, \tau_1} d_{e_G \tau_1, \tau_2} d_{e_G, \tau_1 \tau_2}^{-1} \\
 &= d_{e_G, \tau_1} d_{e_G, \tau_1 \tau_2}^{-1} d_{\tau_1, \tau_2} \quad A \text{ is abelian.} \\
 &= d_{e_G, e_G} d_{e_G, e_G}^{-1} d_{\tau_1, \tau_2} \quad \text{assumption} \\
 &= d_{\tau_1, \tau_2}
 \end{aligned}$$

This proves that $\mathcal{A}$ is a group action.

Remark The set on which G acts, can be taken as the free group generated by $G \times G$, then, there is a group homomorphism from this free group into A , sending the generators to their images in A . However for the group action to be a group homomorphism, maybe an additional condition is required.

Lemma 113 (*Group action on A and extension isomorphisms induced by a function*) A function $c : G \times G \rightarrow A$, determines a group action on E extending action on A which is a normal subgroup of E such that $G \cong E/A$ if and only if it satisfies

$$c(gh, x) = g(c(h, x))c(g, x),$$

for a section $s : G \rightarrow E$ of $\pi : E \rightarrow G \cong G/A$,

$$g(s(x)) = c(g, x)s(x)$$

that extends the action on A . Furthermore for each $g \in G$ $c(g, -) : G \rightarrow A$ determines an extension isomorphic to the first.

In order to determine a group action,

$$\begin{aligned}
 c(gh, x)s(x) &= (gh)(s(x)) = g(h(s(x))) = g(c(h, x)s(x)) = g(c(h, x))g(s(x)) \\
 &= g(c(h, x))c(g, x)s(x)
 \end{aligned}$$

i.e.

$$c(gh, x) = g(c(h, x))c(g, x)$$

and

$$c(e_G, x) = e_A.$$

On the other hand, letting $g = e_G$ (or $h = e_G$) in the first equation implies the second.

For each g fixed, assuming that g extends to a group homomorphism through this definition:

$$g(s(x)s(y)s(xy)^{-1}) = g(d_{x,y}) = s(g)d_{x,y}s(g)^{-1}.$$

So then:

$$c(g, x)s(x)c(g, y)s(y)(c(g, xy)s(xy))^{-1} = s(g)d_{x,y}s(g)^{-1},$$

i.e

$$c(g, x)s(x)c(g, y)s(x)^{-1}s(x)s(y)s(xy)^{-1}c(g, xy)^{-1} = s(g)d_{x,y}s(g)^{-1},$$

i.e.

$$c(g, x)\mathcal{A}(x, c(g, y))d_{x,y}c(g, xy)^{-1} = \mathcal{A}(g, d_{x,y})$$

By above, and previous lemma, $g(d_{x,y})$ determines an extension, isomorphic to the first, for each g .

Lemma 114 *Suppose a group G acts on a group E and for all $\sigma \in G$, the normal subgroup A of E is mapped into itself. i.e. $\sigma(A) = A$. Then G acts on E/A . The action is trivial if and only if $\sigma(x)x^{-1} \in A$, i.e. $\pi(\sigma(x)) = \sigma(x)$.*

Since $\sigma(A) = A$, we have that $\sigma(xA) = \sigma(x)A$. Since $\sigma(xA) = xA$ if and only if $\sigma(x)A = xA$ i.e. if and only if $x^{-1}\sigma(x) \in A$. By normality of A that is equivalent to $\sigma(x)x^{-1} \in A$, which is equivalent to the last condition.

The following two theorems restate the lemmas proved so far.

Theorem 23 *If A is an abelian group, and G is a group that acts on A , and there exist maps*

$d : G \times G \rightarrow A$ and $c : G \times G \rightarrow A$ satisfying:

(1)

$$\tau_1(d_{\tau_2, \tau_3})d_{\tau_1, \tau_2 \tau_3} = d_{\tau_1, \tau_2}d_{\tau_1 \tau_2, \tau_3}$$

(2)

$$c_{\rho\sigma}(\tau) = \rho(c_\sigma(\tau))c_\rho(\tau)$$

and

(3)

$$d_{\tau_1, \tau_2}c_\rho(\tau_1)\tau_1(c_\rho(\tau_2)) = \rho(d_{\tau_1, \tau_2})c_\rho(\tau_1\tau_2)$$

then there exists an extension E of G by A and extension automorphisms of E indexed by G and a group action of G on E that extends the action on A , defined by

$$\rho(s(\tau)) = c(\rho, \tau)s(\tau),$$

for a section $s : G \rightarrow E$ that fits with d .

Theorem 24 Furthermore if only the first condition is satisfied, then there exists an extension E of G by A , and if there exists an action of G on E extending the action on A , such that $\pi(g(x)) = \pi(x)$, then a function $c : G \times G \rightarrow A$ satisfying the other properties defined by $c(\sigma, \tau) = \sigma(s(\tau))s(\tau)^{-1}$ exists, where $s : G \rightarrow E$, is a section, such that $d_{\tau_1, \tau_2} = s(\tau_1)s(\tau_2)s(\tau_1\tau_2)^{-1}$

Existence of extension By Lemma titled "Existence of extension and section compatible with d ", once first equation is satisfied we know that there is an extension and a section that fits with d .

Group Action's existence By Lemma titled "Group action on A and extension isomorphisms induced by a function", once second equation is satisfied we know that there is a group action. To repeat the argument here: Assume that

$$\rho(s(\tau)) = c_\rho(\tau)s(\tau)$$

and more generally

$$\rho(\iota(a)s(\tau)) = \iota(\rho(a))\rho(s(\tau))$$

defines a function on $G \times E \rightarrow E$. We want to show that this is a group action. First condition:

$$\sigma(\rho(x)) = (\sigma\rho)(x)$$

must hold for all $x \in E$. But it already holds on A , so it suffices to check that it holds on section elements.

$$(\sigma\rho)(s(\tau)) = c(\sigma\rho, \tau)s(\tau)$$

and the left hand side, by using the proposed definition for action and by using equation (2) can be evaluated as:

$$\begin{aligned} \sigma(\rho(s(\tau))) &= \sigma(c_\rho(\tau)s(\tau)) \\ &= \sigma(c_\rho(\tau))\sigma(s(\tau)) \\ &= \sigma(c_\rho(\tau))c_\sigma(\tau)s(\tau) \\ &= c_{\sigma\rho}(\tau)s(\tau) \end{aligned}$$

Second condition:

$$e_G(x) = x$$

for all $x \in E$. Again it suffices to check on section elements.

$$e_G(s(\tau)) = c(e_G, \tau)s(\tau)$$

But by equation (2) with $\rho = e_G$ we have

$$c_\sigma(\tau) = e_G(c_\sigma(\tau))c_{e_G}(\tau)$$

Since G' action on A is a group action $e_G(a) = a$, so we have

$$c_\sigma(\tau) = c_\sigma(\tau)c_{e_G}(\tau)$$

By cancelling $c_\sigma(\tau)$ we get

$$c_{e_G}(\tau) = e_A,$$

so that

$$e_G(s(\tau)) = s(\tau).$$

Whether for each ρ this is a group homomorphism of E , i.e.

$$\rho((a_1, \tau_1)(a_2, \tau_2)) = \rho((a_1, \tau_1))\rho((a_2, \tau_2))$$

equivalently

$$\rho(\iota(a_1)s(\tau_1)\iota(a_2)s(\tau_2)) = \rho(\iota(a_1)s(\tau_1))\rho(\iota(a_2)s(\tau_2))$$

Since

$$\begin{aligned} \iota(a_1)s(\tau_1)\iota(a_2)s(\tau_2) &= \iota(a_1)s(\tau_1)\iota(a_2)s(\tau_1)^{-1}s(\tau_1)s(\tau_2)s(\tau_1\tau_2)^{-1}s(\tau_1\tau_2) \\ &= \iota(a_1)\tau_1(\iota(a_2))d_{\tau_1,\tau_2}s(\tau_1\tau_2) \end{aligned}$$

Left hand side evaluates to

$$\begin{aligned} \rho(\iota(a_1)s(\tau_1)\iota(a_2)s(\tau_2)) &= \rho(\iota(a_1)\tau_1(\iota(a_2))d_{\tau_1,\tau_2}s(\tau_1\tau_2)) \\ &= \rho(\iota(a_1\tau_1(a_2)d_{\tau_1,\tau_2}))\rho(s(\tau_1\tau_2)) \\ &= \rho(\iota(a_1\tau_1(a_2)d_{\tau_1,\tau_2}))c_\rho(\tau_1\tau_2)s(\tau_1\tau_2) \\ &= \rho(a_1)\rho(\tau_1(a_2))\rho(d_{\tau_1,\tau_2})c_\rho(\tau_1\tau_2)s(\tau_1\tau_2) \end{aligned}$$

Right-hand side evaluates to

$$\begin{aligned}
 \rho(\iota(a_1)s(\tau_1))\rho(\iota(a_2)s(\tau_2)) &= \rho(a_1)c_\rho(\tau_1)s(\tau_1)\rho(a_2)c_\rho(\tau_2)s(\tau_2) \\
 &= \rho(a_1)c_\rho(\tau_1)s(\tau_1)\rho(a_2)c_\rho(\tau_2)s(\tau_1)^{-1}s(\tau_1)s(\tau_2)s(\tau_1\tau_2)^{-1}s(\tau_1\tau_2) \\
 &= \rho(a_1)c_\rho(\tau_1)\tau_1(\rho(a_2)c_\rho(\tau_2))d_{\tau_1,\tau_2}s(\tau_1\tau_2) \\
 &= \rho(a_1)c_\rho(\tau_1)\tau_1(\rho(a_2))\tau_1(c_\rho(\tau_2))d_{\tau_1,\tau_2}s(\tau_1\tau_2) \\
 &= \rho(a_1)\tau_1(\rho(a_2))d_{\tau_1,\tau_2}c_\rho(\tau_1)\tau_1(c_\rho(\tau_2))s(\tau_1\tau_2) \\
 &= \rho(a_1)\tau_1(\rho(a_2))\rho(d_{\tau_1,\tau_2})c_\rho(\tau_1\tau_2)s(\tau_1\tau_2) \quad \text{Equation (3)}
 \end{aligned}$$

If ρ and τ_1 commute then we are done. However this need not be the case.

Whether for each ρ this is a set automorphism of E ,

$$\rho(\iota(a)s(\tau)) = \iota(\rho(a))\rho(s(\tau)) = \iota(\rho(a))c_\rho(\tau)s(\tau)$$

If

$$\rho(a_1)c_\rho(\tau_1)s(\tau_1) = \rho(a_2)c_\rho(\tau_2)s(\tau_2)$$

By applying π on both sides, we see that $\tau_1 = \tau_2$. By cancelling $c_\rho(\tau_1)s(\tau_1) = c_\rho(\tau_2)s(\tau_2)$ from both sides we get:

$$\rho(a_1) = \rho(a_2)$$

But then $a_1 = a_2$.

Extension-Isomorphism By lemma Group action on A and extension isomorphisms induced by a function, equation (2) suffices for us to conclude that c_g determine extension isomorphisms.

Remark It seems contradictory that the actions do not necessarily introduce group automorphisms yet be extension isomorphisms. Therefore either we are forced to accept

commutativity of action, or resolve this situation some other way.

Equation (3) is implied by (2) and action definition if ρ is a homomorphism.

$$(3) \ d_{\tau_1, \tau_2} c_\rho(\tau_1) \tau_1(c_\rho(\tau_2)) = \rho(d_{\tau_1, \tau_2}) c_\rho(\tau_1 \tau_2)$$

$$(2) \ c_{\rho\sigma}(\tau) = \rho(c_\sigma(\tau)) c_\rho(\tau)$$

and

$$(A) \ \rho(s(\tau)) = c(\rho, \tau) s(\tau),$$

$$\begin{aligned} \rho(d_{\tau_1, \tau_2}) c_\rho(\tau_1 \tau_2) &= \rho(d_{\tau_1, \tau_2}) \rho(s(\tau_1 \tau_2)) s(\tau_1 \tau_2)^{-1} \text{ by (A)} \\ &= \rho(d_{\tau_1, \tau_2} s(\tau_1 \tau_2)) s(\tau_1 \tau_2)^{-1} \\ &= \rho(s(\tau_1) s(\tau_2)) s(\tau_1 \tau_2)^{-1} \text{ by } d \text{ in terms of } s \\ &= \rho(s(\tau_1)) \rho(s(\tau_2)) s(\tau_1 \tau_2)^{-1} \text{ if } \rho \text{ is a homomorphism.} \\ &= c_\rho(\tau_1) s(\tau_1) c_\rho(\tau_2) s(\tau_2) s(\tau_1 \tau_2)^{-1} \text{ by (2)} \\ &= c_\rho(\tau_1) s(\tau_1) c_\rho(\tau_2) s(\tau_1)^{-1} s(\tau_1) s(\tau_2) s(\tau_1 \tau_2)^{-1} \\ &= c_\rho(\tau_1) \tau_1(c_\rho(\tau_2)) d_{\tau_1, \tau_2} \\ &= c_\rho(\tau_1) \tau_1(c_\rho(\tau_2)) d_{\tau_1, \tau_2} \end{aligned}$$

For the questionable step:

$$\begin{aligned}
 \rho(s(\tau_1)s(\tau_2)) &= \rho(d_{\tau_1, \tau_2}s(\tau_1\tau_2)) \\
 &= \rho(d_{\tau_1, \tau_2})\rho(s(\tau_1\tau_2)) \\
 &= \rho(d_{\tau_1, \tau_2})c_\rho(\tau_1\tau_2)s(\tau_1\tau_2) \text{ by (A)}
 \end{aligned}$$

$$\begin{aligned}
 \rho(s(\tau_1))\rho(s(\tau_2)) &= c_\rho(\tau_1)s(\tau_1)c_\rho(\tau_2)s(\tau_2) \\
 &= c_\rho(\tau_1)s(\tau_1)c_\rho(\tau_2)s(\tau_1)^{-1}s(\tau_1)s(\tau_2) \\
 &= c_\rho(\tau_1)\tau_1(c_\rho(\tau_2))d_{\tau_1, \tau_2}s(\tau_1\tau_2) \\
 &= c_\rho(\tau_1)c_{\tau_1\rho}(\tau_2)c_{\tau_1}(\tau_2)^{-1}d_{\tau_1, \tau_2}s(\tau_1\tau_2) \text{ by (2)}
 \end{aligned}$$

8.11. EXACT SEQUENCES WITH RELATIVE WEIL GROUPS, LOCAL AND GLOBAL

Let ν be a valuation of $\bar{\mathbb{Q}}$ and hence of $\mathbb{Q}$, and $\mathbb{Q}_\nu$ and $\bar{\mathbb{Q}}_\nu$ be completions of $\mathbb{Q}$ and $\bar{\mathbb{Q}}$ with respect to ν . Eventually ν will be defined by inclusion $\bar{\mathbb{Q}} \subset \mathbb{C}$ and $\mathbb{Q}_\nu$ will be $\mathbb{R}$ and $\bar{\mathbb{Q}}_\nu$ will be $\mathbb{C}$.

In any case, there are embeddings

$$F_\nu^\times \hookrightarrow C_F$$

and

$$\text{Gal}(F_\nu/\mathbb{Q}_\nu) \hookrightarrow \text{Gal}(F/\mathbb{Q})$$

if F is any finite Galois extension of $\mathbb{Q}$ in $\bar{\mathbb{Q}}$

Local and global Weil groups $W_{F_\nu/\mathbb{Q}_\nu}$ and $W_{F/\mathbb{Q}}$ are defined as extensions fitting into a commutative diagram:

$$\begin{array}{ccccccc} 1 & \longrightarrow & F_\nu^\times & \longrightarrow & W_{F_\nu/\mathbb{Q}_\nu} & \longrightarrow & \text{Gal}(F_\nu/\mathbb{Q}_\nu) \longrightarrow 1 \\ & & \downarrow & & \downarrow I_F & & \downarrow \\ 1 & \longrightarrow & C_F & \longrightarrow & W_{F/\mathbb{Q}} & \longrightarrow & \text{Gal}(F/\mathbb{Q}) \longrightarrow 1 \end{array}$$

where central arrows can be chosen compatible with field extensions so that upon passage to the limit yield $I : W_{\mathbb{Q}_\nu} \rightarrow W_{\mathbb{Q}}$. It is the image of $W_{\mathbb{Q}_\nu}$ in $W_{\mathbb{Q}}$ that will be fixed. I_F may be changed to $w \mapsto x I_F(w) x^{-1}$ where $x \in C_F$ and $x \sigma(x)^{-1} \in F_\nu^\times$ for all $\sigma \in \text{Gal}(F_\nu/\mathbb{Q}_\nu)$.

8.12. LANGLANDS' CONSTRUCTION OF TANIYAMA GROUP, MAP FROM WEIL GROUP TO TANIYAMA GROUP

This section follows [60] and [66].

Let ι be complex conjugation, or the nontrivial element of $\text{Gal}(\mathbb{C}/\mathbb{R})$, or complex conjugation as an element of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

For this section we are assuming existence of Serre group $\mathcal{S}$ which satisfies an extension, and whose character group is given by

$$X^*(\mathcal{S}) = \{\lambda \in M \mid (1 + \iota)(1 - \sigma)\lambda = 0 \text{ for all } \sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\}$$

where M is the locally constant integer-valued functions on $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and Galois group acting by right translation on M .

For a finite Galois extension L of $\mathbb{Q}$, let $\mathcal{S}^L$ be the quotient group of $\mathcal{S}$ whose lattice of rational characters consists of all functions in $X^*(\mathcal{S})$ invariant under $\text{Gal}(\bar{\mathbb{Q}}/L)$, i.e.

$$X^*(\mathcal{S}^L) = (X^*(\mathcal{S}))^{\text{Gal}(\bar{\mathbb{Q}}/L)}$$

We are also assuming existence of an extension, defining the Taniyama group, with a splitting over adeles.

Let ν be the valuation given by $\bar{\mathbb{Q}} \subset \mathbb{C}$. Let $F_\infty^\times = \prod_{w|\nu} F_w$.

$F_\infty^\times \rightarrow I_F \rightarrow C_F$ is an embedding. (Note $F_\infty^\times \cap F^\times = \{1\}$.)

Let $\tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and $w = w(\tau) \in W_{L/\mathbb{Q}}$, be the element obtained by lifting τ to $W_{\mathbb{Q}}$ and projecting to $W_{L/\mathbb{Q}}$.

$$\begin{array}{ccc}
 \ker(\varphi) & & C_L \\
 \downarrow & & \downarrow \\
 W_{\mathbb{Q}} & \xrightarrow{\pi} & W_{L/\mathbb{Q}} \\
 \downarrow \varphi & & \downarrow \\
 \tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & \text{Gal}(L/\mathbb{Q})
 \end{array}$$

where $\ker \varphi$ is the connected component of identity, isomorphic to the inverse limit, under the norm maps $N_{E/E'}$ of the connected components D_E of 1 in C_E . These norm maps $D_E \rightarrow D_{E'}$ are surjective, and $r_E(D_E) = (\text{Ker } \varphi)W_E^c/W_E^c$ is the image of $\text{Ker } \varphi$ in $W_{E/\mathbb{Q}}$. (This is from Tate's number theoretic background.) here $\mathbb{Q} \subseteq E' \subseteq E \subseteq \bar{\mathbb{Q}}$.

Therefore $\pi(\ker \varphi) = \iota_L(D_L)$, where D_L is the connected component of identity in C_L . (and $\iota : W_L^{\text{ab}} \rightarrow W_{L/\mathbb{Q}}$ is inclusion.)

Therefore $w(\tau)$ is well-defined modulo the connected component D_L , in particular modulo the closure of $L_{\infty}^{\times}$. ($L_{\infty}^{\times} \supset D_L$?)

Lemma 115 *There exists a set of representatives w_{σ} for $\sigma \in \text{Gal}(L/\mathbb{Q})$ for the cosets of C_L in $W_{L/\mathbb{Q}}$, such that the following holds:*

(SC1) $w_1 = 1$.

(SC2) If $\sigma \in \text{Gal}(L_{\nu}/\mathbb{Q}_{\nu})$ then $w_{\sigma} \in W_{L_{\nu}/\mathbb{Q}_{\nu}}$.

(SC3) If $\rho \in \text{Gal}(L/\mathbb{Q})$ and $\sigma \in \text{Gal}(L_{\nu}/\mathbb{Q}_{\nu})$, then $a_{\rho,\sigma} = w_{\rho}w_{\sigma}w_{\rho\sigma}^{-1} \in L_{\infty}^{\times}$.

(SC4) For $\mathfrak{f}$ being a choice of representatives of cosets of $\text{Gal}(L/\mathbb{Q})/\text{Gal}(L_{\nu}/\mathbb{Q}_{\nu})$, that contains 1, then for $a_{\rho,\sigma} = w_{\rho}w_{\sigma}w_{\rho\sigma}^{-1}$, whenever $\eta \in \mathfrak{f}$, and $\sigma \in \text{Gal}(L_{\nu}/\mathbb{Q}_{\nu})$ then $a_{\eta,\sigma} = 1$.

Proof

Note that

$$\text{Gal}(L/\mathbb{Q}) = \{\eta\sigma \mid \eta \in \mathfrak{f} \sigma \in \text{Gal}(L_{\nu}/\mathbb{Q}_{\nu})\}$$

Then after choosing w_σ to satisfy condition (SC2), and setting w_η , simply choose $w_{\eta\sigma} = w_\eta w_\sigma$.

canonical coweight For canonical isomorphism $h : \mathcal{R} \rightarrow S$, where S is the Serre group, and over $\mathbb{C}$, $\mathcal{R} = \mathrm{GL}(1) \times \mathrm{GL}(1)$ is the restriction of scalars $\mathrm{Res}_{\mathbb{C}/\mathbb{R}}$.

Restriction of h to the first factor is the canonical coweight $\mu : \mathbb{C}^\times \rightarrow S$. or $(\mu : G_m \rightarrow S)$ i.e. $\mu \in X_*(S)$. and is identified also as a coweight of $\mathcal{S}^L$ which is a quotient of S .

Definition of coweight operation

For $\nu \in X_*(\mathcal{S}^L)$, and x an invertible element of L or of $\mathbb{A}_f(L)$, x^ν element of $\mathcal{S}^L(L)$, or $\mathcal{S}^L(\mathbb{A}_f(L))$ satisfying

$$\lambda(x^\nu) = x^{\langle \lambda, \nu \rangle} \quad \lambda \in X^*(\mathcal{S}^L)$$

Here

$$X_*(\mathcal{S}^L) = \mathrm{Hom}(X^*(\mathcal{S}^L), \mathbb{Z})$$

where $\nu(\lambda) = \langle \lambda, \nu \rangle \in \mathbb{Z}$. And also $X_*(\mathcal{S}^L) = \mathrm{Hom}(G_m, \mathcal{S}^L)$. Under this interpretation, the composition $\lambda \circ \nu : G_m \rightarrow G_m$ is given by $\lambda \circ \nu(x) = x^{\langle \lambda, \nu \rangle}$. In case of ideles, $G_m(A_f(L))$ lies in a product of $G_m(L_v)$ for valuations v of L hence the same formula holds.

Definition of b_0

For $w \in W_{L/\mathbb{Q}}$ and w_σ chosen to satisfy the four conditions (SC1-4), let

$$c_\sigma(w) = w_\sigma w w_{\sigma\tau}^{-1}.$$

For $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and $w = w(\tau) \in W_{L/\mathbb{Q}}$, obtained by lifting τ to $W_{\mathbb{Q}}$ and projecting. (This was already mentioned above.) i.e.

$$w \in \pi\varphi^{-1}(\tau).$$

Then $c_\sigma(w) \in C_L$.

Then let

$$b_0(\tau) = \prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} c_\sigma(w)^{\sigma\mu} \in C_L \otimes X_*(\mathcal{S}^L)$$

Lemma 116 For a coset representative choice in $W_{L/\mathbb{Q}}$ of C_L satisfying (SC1-4) $b_0(\tau)$ is well-defined modulo $L_\infty^\times \otimes X_*(\mathcal{S}^L)$

Independence of choice of w

The choices for w , as argued before, differ by an element in the closure of $L_\infty^\times$.

On a subgroup U of the units of L

it is claimed that

$$\prod_{\sigma \in ?} \sigma(v)^{\sigma\nu} = 1$$

for all $v \in U$.

Since $c_\sigma(uw) = \sigma(u)c_\sigma(w)$ (Note $w_\sigma u w w_{\sigma\tau}^{-1} = w_\sigma u w_\sigma^{-1} w_\sigma w w_{\sigma\tau} = \sigma(u)c_\sigma(w)$)

b_0 defined by uw or w are congruent, for $u \in U$.

If $u = \lim_n u_n$ where $u_n \in L_\infty^\times U$, then for the choice of $u_n w$ and w , the corresponding b'_0 s are congruent, hence the same holds in the limit.

Independence of section If representatives w_σ are replaced by $e_\sigma w_\sigma$ with $e_\sigma \in C_L$, and w'_σ still satisfy the same conditions, then

(i) If $\sigma \in \text{Gal}(L_v/\mathbb{Q}_v)$, then $e_\sigma \in L_v^\times$, by (SC2). Furthermore $\rho(e_\sigma) \in L_\infty^\times$. for $\rho \in \text{Gal}(L/\mathbb{Q})$, since Galois group action sends an infinite prime to another infinite prime.

But

$$a'_{\rho,\sigma} = (e_\rho w_\rho)(e_\sigma w_\sigma)(e_{\rho\sigma} w_{\rho\sigma})^{-1} = e_\rho w_\rho e_\sigma w_\rho^{-1} a_{\rho,\sigma} e_{\rho\sigma}^{-1} = e_\rho \rho(e_\sigma) e_{\rho\sigma}^{-1} a_{\rho,\sigma}.$$

Since $a'_{\rho,\sigma}$ and $a_{\rho,\sigma}$ must both lie in $L_\infty^\times$ by (SC3), e_ρ and $e_{\rho\sigma}$ must be congruent modulo $L_\infty^\times$, for $\sigma \in \text{Gal}(L_v/\mathbb{Q}_v)$.

(ii) Also:

$$\begin{aligned}
 c'_\sigma(w) &= w'_\sigma w (w'_{\sigma\tau})^{-1} \\
 &= e_\sigma w_\sigma w (e_{\sigma\tau} w_{\sigma\tau})^{-1} \\
 &= e_\sigma w_\sigma w w_{\sigma\tau}^{-1} e_{\sigma\tau}^{-1} \\
 &= e_\sigma c_\sigma(w) e_{\sigma\tau}^{-1} \\
 &= e_\sigma e_{\sigma\tau}^{-1} c_\sigma(w)
 \end{aligned}$$

where commutativity of C_L is used in the last step.

Then

$$b'_0(\tau) = \left(\prod_\sigma (e_\sigma e_{\sigma\tau}^{-1})^{\sigma\mu} \right) b_0(\tau)$$

where we utilize that

$$(xy)^{\sigma\mu} = x^{\sigma\mu} y^{\sigma\mu}$$

and

$$(x^{-1})^{\sigma\mu} = (x^{\sigma\mu})^{-1}$$

is utilized below:

But note that

$$\begin{aligned}
\prod_{\sigma} (e_{\sigma} e_{\sigma\tau}^{-1})^{\sigma\mu} &= \prod_{\sigma} e_{\sigma}^{\sigma\mu} (e_{\sigma\tau}^{\sigma\mu})^{-1} \\
&= \left(\prod_{\sigma} e_{\sigma}^{\sigma\mu} \right) \left(\prod_{\sigma} (e_{\sigma\tau}^{\sigma\mu})^{-1} \right) \\
&= \left(\prod_{\sigma} e_{\sigma}^{\sigma\mu} \right) \left(\prod_{\sigma} (e_{\sigma}^{\sigma\tau^{-1}\mu})^{-1} \right) \\
&= \prod_{\sigma} e_{\sigma}^{\sigma\mu - \sigma\tau^{-1}\mu} \\
&= \prod_{\sigma} e_{\sigma}^{\sigma(1-\tau^{-1})\mu}
\end{aligned}$$

But now note that each $\sigma \in \text{Gal}(L/\mathbb{Q})$ may be written as $\eta\sigma'$ with $\sigma' \in \text{Gal}(L_v/\mathbb{Q}_v)$, and $\eta \in \mathfrak{f}$, so

$$= \prod_{\eta} \prod_{\sigma'} e_{\eta\sigma'}^{\eta\sigma'(1-\tau^{-1})\mu}$$

Utilizing that $e_{\eta\sigma'}$ and e_{η} are congruent modulo $L_{\infty}^{\times}$, (this is conclusion of (i)) above may be rewritten as

$$\begin{aligned}
&= \prod_{\eta} \prod_{\sigma'} e_{\eta}^{\eta\sigma'(1-\tau^{-1})\mu} \\
&= \prod_{\eta} e_{\eta}^{\eta \sum_{\sigma'} \sigma'(1-\tau^{-1})\mu}
\end{aligned}$$

But

$$\sum_{\sigma' \in \text{Gal}(L_v/\mathbb{Q}_v)} \sigma'(1-\tau^{-1})\mu = (1+\iota)(1-\tau^{-1})\mu = 0$$

where we utilize a property of trace for the first equality $\sum_{\sigma'} \sigma' = 1 + \iota$ and the last equality

comes from the fact that for $\lambda \in X^*(\mathcal{S})$, we have

$$(1 + \iota)(1 - \sigma)\lambda = 0$$

for all $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. and the same property can be transferred to coweights in $X_*(\mathcal{S})$

Note that we switched to additive notation, where on the group of coweights interpreted as a Galois-module, addition means, performing the group operation in the image, and $x \mapsto x^{-1}$ corresponds to the coweight -1 , and 0 is the coweight that maps everything to identity.

Therefore $b'_0(\tau)$ and $b_0(\tau)$ are the same modulo $L_\infty^\times$.

Independence from choice of $I : W_{L_v/\mathbb{Q}_v} \rightarrow W_{L/\mathbb{Q}}$

I_L may be changed to $w \mapsto xI_L(w)x^{-1}$ where $x \in C_L$ and $x\sigma(x)^{-1} \in L_v^\times$ for all $\sigma \in \text{Gal}(L_v/\mathbb{Q}_v)$ (The first part is number theoretic background, automorphisms of Weil group.) That $x\sigma(x)^{-1} \in L_v^\times$.

Note the assumption (SC3) at least implies that

$$a'_{\rho,\sigma} \in L_\infty,$$

so that

$$w_\rho x w_\sigma x^{-1} w_{\rho\sigma}^{-1} = \rho(x)(\rho\sigma)(x^{-1})a_{\rho\sigma} \in L_\infty.$$

so that $\rho(x\sigma(x)^{-1}) \in L_\infty$

Assuming this condition holds (why later), then changing I_L will change $b_0(\tau)$ by changing $c_\sigma(w) = w_\sigma w w_{\sigma\tau}^{-1}$, when $\sigma \in \text{Gal}(L_\nu/\mathbb{Q}_{nu})$, by (SC2) $w_\sigma \in W_{L_\nu/\mathbb{Q}_\nu}$, hence in computing $c_\sigma(w)$, it may be changed to

$$c'_\sigma(w) = x w_\sigma x^{-1} w w_{\sigma\tau}^{-1} = x\sigma(x)^{-1} c_\sigma(w)$$

(Here $\sigma\tau \notin \text{Gal}(L_\nu/\mathbb{Q}_\nu)$, in general, and if it were, then the last term also would change.)

By assumption $x\sigma(x)^{-1} \in L_\nu^\times \subset L_\infty^\times$, therefore this does not change b_0 If w is changed to xwx^{-1} then

$$c'_\sigma(w) = w_\sigma x w x^{-1} w_{\sigma\tau}^{-1} = w_\sigma x w x^{-1} w^{-1} w_\sigma^{-1} w_\sigma w w_{\sigma\tau}^{-1} = \sigma(x\tau(x^{-1})) c_\sigma(w)$$

(Image of τ in $\text{Gal}(L/\mathbb{Q})$ and τ are identified.) Then in the overall contribution:

$$\begin{aligned}
 b'_0(\tau) &= \prod_{\sigma} c'_{\sigma}(w)^{\sigma\mu} \\
 &= \prod_{\sigma} (\sigma(x)\sigma\tau(x^{-1})c_{\sigma}(w))^{\sigma\mu} \\
 &= \prod_{\sigma} (\sigma(x)\sigma\tau(x^{-1}))^{\sigma\mu} b_0(\tau)
 \end{aligned}$$

Now the differing factor

$$\begin{aligned}
 \prod_{\sigma} (\sigma(x)\sigma\tau(x^{-1}))^{\sigma\mu} &= \prod_{\sigma} \sigma(x)^{\sigma\mu} \prod_{\sigma} (\sigma\tau(x^{-1}))^{\sigma\mu} \\
 &= \prod_{\sigma} \sigma(x)^{\sigma\mu} \prod_{\sigma} (\sigma(x^{-1}))^{\sigma\tau^{-1}\mu} \\
 &= \prod_{\sigma} \sigma(x)^{\sigma\mu - \sigma\tau^{-1}\mu} \\
 &= \prod_{\sigma} \sigma(x)^{\sigma(1-\tau^{-1})\mu} \\
 &= \prod_{\eta} \prod_{\sigma'} (\eta(x)\sigma'(x))^{\eta\sigma'(1-\tau^{-1})\mu} \\
 &= \prod_{\eta} \prod_{\sigma'} (\eta(x)x)^{\eta\sigma'(1-\tau^{-1})\mu}
 \end{aligned}$$

Here $\sigma'(x)$ may be replaced by x because by assumption $x\sigma(x)^{-1} \in L_\nu^\times \subset L_\infty^\times$. then

$$\begin{aligned} &= \prod_{\eta} (\eta(x)x)^{\eta \sum_{\sigma'} \sigma'(1-\tau^{-1})\mu} \\ &= \prod_{\eta} (\eta(x)x)^{\eta(1+\iota)(1-\tau^{-1})\mu} \end{aligned}$$

Then as in previous case, $(1+\iota)(1-\tau^{-1})\mu = 0$, so the above evaluates to identity, hence b_0 is unchanged.

Finally replacements for $w_{\sigma\tau}$ could also occur. If $\sigma\tau = \eta_1\sigma_1$, then $w_{\sigma\tau} = w_{\eta_1}w_{\sigma_1}$ where w_{σ_1} could be replaced by $xw_{\sigma_1}x^{-1}$. Then

$$w'_{\sigma\tau} = w_{\eta_1}w_{\sigma_1}w_{\sigma_1}^{-1}xw_{\sigma_1}x^{-1} = w_{\sigma\tau}(\sigma_1)^{-1}(x)x^{-1}$$

hence

$$(w'_{\sigma\tau})^{-1} = x(\sigma_1)^{-1}(x^{-1})w_{\sigma\tau}^{-1} = w_{\sigma\tau}^{-1}\sigma\tau(x(\sigma_1)^{-1}(x^{-1}))$$

This yields that

$$c'_\sigma(w) = c_\sigma(w)\sigma\tau(x(\sigma_1)^{-1}(x^{-1})) = c_\sigma(w)\eta_1(\sigma_1(x)x^{-1})$$

Note that as σ varies over $\text{Gal}(L/\mathbb{Q})$, then $\sigma\tau$ also varies over the whole set, and η_1, σ_1 vary over all choices.

By assumption that $\sigma_1(x)x^{-1} \in L_\infty$, then the product forming b_0 is unaffected.

Then

$$\prod_{\sigma} (\sigma\tau(x(\sigma_1)^{-1}(x^{-1})))^{\sigma\mu} = \prod_{\eta_1, \sigma_1} (\eta_1(\sigma_1(x)x^{-1}))^{\eta_1\sigma_1\tau^{-1}\mu}$$

remark The influence of changing I on w_σ and $w_{\sigma\tau}$ can be seen as nothing different than changing coset representatives, hence reduces to the part already considered. The influence on w needs to be considered separately, and this has been done above as well.

Lemma 117 *If $L \subseteq L'$, then $\iota(b_0^{L'}(\tau)) = b_0^L(\tau)$ where $\iota : C_{L'} \otimes X_*(\mathcal{S}^{L'}) \rightarrow C_L \otimes X_*(\mathcal{S}^L)$*

is canonical mapping.

Case $L_\nu = \mathbb{C}$.

In this case $\text{Gal}(L'/L) \cap \text{Gal}(L'_\nu/\mathbb{Q}_\nu) = \{1\}$, since $\text{Gal}(L'_\nu/\mathbb{Q}_\nu) = \text{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \iota\}$, and $\iota \notin \text{Gal}(L'/L)$, since $\text{Gal}(L'/L) \cong \text{Gal}(L'/\mathbb{Q})/\text{Gal}(L/\mathbb{Q})$, and $\iota \in \text{Gal}(L/\mathbb{Q})$, since $L_\nu = \mathbb{C}$.

Let $\mathfrak{e}$ be a set of double-coset representatives of

$$\text{Gal}(L'/L) \backslash \text{Gal}(L'/\mathbb{Q}) / \text{Gal}(L'_\nu/\mathbb{Q}_\nu),$$

so that

$$\text{Gal}(L'/\mathbb{Q}) = \{\zeta\eta\rho \mid \zeta \in \text{Gal}(L'/L), \eta \in \mathfrak{e}, \rho \in \text{Gal}(L'_\nu/\mathbb{Q}_\nu)\}$$

Assume that coset representatives for $\text{Gal}(L'/\mathbb{Q})$ in $W_{L'/\mathbb{Q}}$ satisfy

$$w'_{\zeta\eta\rho} = w'_\zeta w'_\eta w'_\rho$$

and $w'_1 = 1$, and for $\rho \in \text{Gal}(L'_\nu/\mathbb{Q}_\nu)$, we have $w'_\rho \in W_{L'_\nu/\mathbb{Q}_\nu}$, and for $\zeta \in \text{Gal}(L'/L)$ we have $w'_\zeta \in W_{L'/L}$.

Let w' be $w(\tau) \in \pi\varphi^{-1}(\tau)$ for L' (i.e. $\pi : W_{\mathbb{Q}} \rightarrow W_{L'/\mathbb{Q}}$) and w be $w(\tau) \in \pi\varphi^{-1}(\tau)$ for L (i.e. $\pi : W_{\mathbb{Q}} \rightarrow W_{L/\mathbb{Q}}$) Then for $\pi : W_{L'/\mathbb{Q}} \rightarrow W_{L/\mathbb{Q}}$, we have $\pi(w') = w$.

If $\sigma \in \text{Gal}(L/\mathbb{Q})$, then it lifts to a unique element of $\text{Gal}(L'/\mathbb{Q})$ of the form $\eta\rho$ with $\eta \in \mathfrak{e}$ and $\rho \in \text{Gal}(L'_\nu/\mathbb{Q}_\nu)$. (Remark: any lift can be written in the form $\zeta\eta\rho$, but $\pi(\zeta\eta\rho) = \pi(\eta\rho)$, for $\pi : \text{Gal}(L'/\mathbb{Q}) \rightarrow \text{Gal}(L/\mathbb{Q})$.)

Now suppose that

$$\eta\rho\tau = \zeta_1\eta_1\rho_1$$

Then $\pi(\zeta\eta_1\rho_1) = \sigma\tau$ for all ζ .

And also suppose

$$w_\sigma = \pi(w'_\eta w'_\rho)$$

for all σ

Then we have

$$w_{\sigma\tau} = \pi(w'_{\zeta_1} w'_{\eta_1} w'_{\rho_1})$$

And consequently:

$$\begin{aligned} c_\sigma(w) &= w_\sigma w w_{\sigma\tau}^{-1} \\ &= \pi(w'_\eta w'_\rho) \pi(w') \pi(w'_{\rho_1})^{-1} \pi(w'_{\eta_1})^{-1} \pi(w'_{\zeta_1})^{-1} \\ &= \pi(w'_\eta w'_\rho w' (w'_{\rho_1})^{-1} (w'_{\eta_1})^{-1} (w'_{\zeta_1})^{-1}) \\ &= \pi(c_{\eta\rho}(w')) \end{aligned}$$

where in the last step we have utilized that $w'_{\eta\rho} = w'_\eta w'_\rho$ and since $\eta\rho\tau = \zeta_1\eta_1\rho_1$, we also have $w'_{\eta\rho\tau} = w'_{\zeta_1} w'_{\eta_1} w'_{\rho_1}$

On the other hand, as a remark we note that because of the commutativity of the diagram:

$$\begin{array}{ccc} C_{L'} & \longrightarrow & W_{L'/\mathbb{Q}} \\ N_{L'/L} \downarrow & & \downarrow \pi \\ C_L & \longrightarrow & W_{L/\mathbb{Q}} \end{array}$$

means that

$$c_\sigma(w) = \prod_{\sigma_1, \pi(\sigma_1)=\sigma} c_{\sigma_1}(w')$$

by definition of projection on the image of $C_{L'}$ under $r_{L'}$, and noting that

$$\zeta(c_{\eta\rho}(w')) = w'_\zeta c_{\eta\rho}(w') (w'_\zeta)^{-1} = c_{\zeta\eta\rho}(w') w'_{\zeta\zeta_1} (w'_\zeta)^{-1}$$

Note that

$$\prod_{\zeta \in \text{Gal}(L'/L)} w'_{\zeta\zeta_1} (w'_\zeta)^{-1} = 1.$$

either by choice of section, or because we are taking product over all the terms. If we assume

commutativity on $W_{L'/L}$ then the statement is trivially true.

Case $L_\nu = \mathbb{R}$

In this case, $X^*(\mathcal{S}^L) \cong \mathbb{Z}$, and Galois group acts trivially.

(Note $\iota \in \text{Gal}(\bar{\mathbb{Q}}/L)$, because L is contained in a purely real field. Then recall that

$$X^*(\mathcal{S}) = \{\lambda \in M \mid (1 + \iota)(1 - \sigma)\lambda = 0 \text{ for all } \sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\}$$

and

$$X^*(\mathcal{S}^L) = (X^*(\mathcal{S}))^{\text{Gal}(\bar{\mathbb{Q}}/L)}$$

Then assuming ι leaves an element of $X^*(\mathcal{S})$ invariant, implies that $(1 - \sigma)(1 + \iota)\lambda = (1 - \sigma)(2\lambda) = 0$ for all $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, hence $\lambda \in X^*(\mathcal{S}^L)$ if λ is left invariant by Galois group action.)

For the structure of the character group, one possible reference is Serre's book.

In order to argue that the b'_0 defined via L or L' correspond to each other, one considers the cosets:

$$\text{Gal}(L'/L) \backslash \text{Gal}(L'/\mathbb{Q})$$

and argues in a similar way to the previous case.

For a set $\mathfrak{e}$ of coset representatives, every element of $\text{Gal}(L'/\mathbb{Q})$, may be written in the form $\rho\eta$ with $\rho \in \text{Gal}(L'/L)$ and $\eta \in \mathfrak{e}$. We may suppose $w'_{\rho\eta} = w'_\rho w'_\eta$.

If $\sigma \in \text{Gal}(L/\mathbb{Q})$, then $w_\sigma = \pi(w'_\eta)$ where $\pi(\eta) = \sigma$.

The correspondence as in previous case can be established.

Lemma 118 $b(\tau) \in \mathcal{S}^L(\mathbb{A}_f(L))/\mathcal{S}^L(L)$ obtained by projecting any lift $\tilde{b}(\tau) \in \mathcal{S}^L(\mathbb{A}(L)) \cong I_L \otimes X_*(\mathcal{S}^L)$ is well-defined.

This is a direct verification from the definitions, with suitable choice of lifts. It is verified that

$$b(\tau_1)\tau_1(b(\tau_2))b(\tau_1\tau_2)^{-1}$$

lies in $\mathcal{S}^L(L)$.

Lemma 119 $b(\tau)$ satisfies conditions to insure that it defines an extension

$$1 \longrightarrow \mathcal{S}^L \longrightarrow \mathcal{T}^L \longrightarrow \text{Gal}(L^{\text{ab}}/\mathbb{Q}) \longrightarrow 1$$

The coefficients $c_\rho(\tau)$ (not to be confused with those of this section) defined by

$$c_\rho(\tau) = b(\tau)\rho(b(\tau))^{-1}$$

lie in $\mathcal{S}^L(L)$. This is verified.

Lemma 120 $b(\tau)$ depends only on the image of τ in $\text{Gal}(L^{\text{ab}}/\mathbb{Q})$.

Theorem 25 There is a natural homomorphism $\varphi : W_{\mathbb{Q}} \rightarrow \mathcal{T}(\mathbb{C})$ and for any finite extension F of $\mathbb{Q}$ a homomorphism $\varphi_F : W_F \rightarrow \mathcal{T}_F(\mathbb{C})$, defined at finite level via maps $W_{L/\mathbb{Q}} \rightarrow \mathcal{T}^L(\mathbb{C})$.

For coset representatives w_σ satisfying (SC1-3), define for $w \in W_{L/\mathbb{Q}}$,

$$b_0(w) = \prod_{\sigma \in \text{Gal}(L/\mathbb{Q})} c_\sigma(w)^{\sigma\mu}$$

For

$$W_{L/\mathbb{Q}} \rightarrow \text{Gal}(L^{\text{ab}}/\mathbb{Q})$$

defined by pulling back to $W_{\mathbb{Q}}$ and projecting from $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, if τ is the image of w in $\text{Gal}(L^{\text{ab}}/\mathbb{Q})$, then $b_0(w) = b_0(\tau)$ (modulo L_∞ as before.) Then lifting $b_0(w)$ to $b(w)$ in $\mathcal{S}^L(\mathbb{A}(L))$ can be done to insure that projection of $b(w)$ in $\mathcal{S}^L(\mathbb{A}_f(L))$ is $b(\tau)$.

As done in previous lemmas, if τ_i are images of w_i for $i = 1, 2$, then $b(w_1)\tau_1(b(w_2))b(w_1w_2)^{-1} \in \mathcal{S}^L(L)$.

Let $b_\nu(w)$ be projection of $b(w)$ in $\mathcal{S}^L(L_\nu) \cong \mathcal{S}^L(\mathbb{C})$, and define $\varphi(w) = b_\nu(w)a(\tau)$. (where a is a section of the last map in exact sequence defining $\mathcal{T}^L$.)

If coset representatives are changed, then φ is changed to $\text{ad}(a) \circ \varphi$.

9. ARTHUR'S CONSTRUCTION OF LANGLANDS GROUP

9.1. SUMMARY

In “A Note on the Automorphic Langlands Group” [6], James Arthur outlines a tentative construction of Langlands Group.

The indexing set $\mathcal{C}_F$, and extensions of W_F by a compact, semisimple, simply connected Lie group K_c , for each element c of the index set $\mathcal{C}_F$ yields the candidate for Langlands group by taking product over all elements of the index set.

Description of indexing set

Consider pairs (G, c) where G is a quasisplit, simple, simply connected algebraic group over F , and c is a family (or rather an equivalence class of families) in $\mathcal{C}_{\text{prim}}(G)$. Two pairs (G, c) and (G', c') will be said to be isomorphic if there is an isomorphism $G \rightarrow G'$ over F , and a dual isomorphism ${}^L G' \rightarrow {}^L G$ that takes c' to c . $\mathcal{C}_F$ is the set of isomorphism classes of such pairs. The isomorphism class will be denoted by c .

Extension over each element of the indexing set

For $c \in \mathcal{C}_F$, the associated group G , being simply connected, will have a complex dual group $\hat{G}$ of adjoint type. K_c is a compact real form of its simply connected cover $\hat{G}_{\text{sc}}$.

W_F acts on $\hat{G}$, hence on K_c by an action that factors through a finite quotient of the Galois group Γ_F .

In order to define an extension, Arthur constructs a cohomology class to define the extension and the groups in the extension.

Product

Finally L_F is defined as the fibre product

$$L_F = \prod_{c \in \mathcal{C}_F} (L_c \rightarrow W_F)$$

Automorphic Representation Suppose G is a connected reductive algebraic group over F , assumed for simplicity to be quasisplit.

An automorphic representation of G is an irreducible representation π of the adelic group

$G(\mathbb{A})$ that is a constituent of the regular representation of $G(\mathbb{A})$ on $L^2(G(F)\backslash G(\mathbb{A}))$. Being a constituent is formally defined in Langlands' article "On the notion of an automorphic representation" [61].

Any irreducible representation π of $G(\mathbb{A})$ can be written as a restricted tensor product $\pi = \otimes_{\nu} \pi_{\nu}$ of irreducible representations π_{ν} of $G(F_{\nu})$, almost all of which are unramified.

Here a representation is said to be unramified at ν if G is unramified at ν , which means ν is p -adic, and the action of $W_{F_{\nu}}$ on $\hat{G}$ factors through the quotient of $W_{F_{\nu}}$ by the inertia subgroup $I_{F_{\nu}}$.

Conjugacy classes corresponding to automorphic representations

Irreducible representations π_{ν} can be obtained canonically from an induced representation of $G_{F_{\nu}}$, and the inducing data can be represented by a semisimple conjugacy class $c(\pi_{\nu})$ in ${}^L G_{\nu} = \hat{G} \rtimes W_{F_{\nu}}$ that projects to the Frobenius element Frob_{ν} in $W_{F_{\nu}}/I_{F_{\nu}}$ ($I_{F_{\nu}}$ being the inertia subgroup).

For S a finite set of valuations of F outside of which G is unramified, let

$$c^S(\pi) = \{c(\pi_{\nu}) \mid \nu \notin S\}$$

be the family of conjugacy classes $c(\pi_{\nu})$ for those valuations ν outside S .

Let

$$\mathcal{C}_{\text{aut}}^S = \{c^S(\pi) \mid \pi : \text{automorphic representation of } G\}$$

be the set of semisimple conjugacy classes in ${}^L G = \hat{G} \rtimes W_F$ that come from an automorphic representation π of G .

Define an equivalence relation on $\mathcal{C}_{\text{aut}}^S$ by letting $c^S(\pi) \equiv d^S(\pi')$ if the images $c_{\nu} = c(\pi_{\nu})$ and $d_{\nu} = d(\pi'_{\nu})$ in ${}^L G_{\nu}/I_{F_{\nu}}$ are equal for almost all ν . (Can the finite sets be also different in defining the equivalence relation, so that this is defined over $\cup_S \mathcal{C}_{\text{aut}}^S(G)$?)

Let $\mathcal{C}_{\text{aut}}(G)$ denote the set of equivalence classes. (This is independent of S .)

Primitive conjugacy classes

In $\mathcal{C}_{\text{aut}}(G)$ there is a subset called $\mathcal{C}_{\text{prim}}(G)$, which is the set of primitive families. This is defined by the following condition, $c \in \mathcal{C}_{\text{aut}}(G)$ is primitive for any representation r of ${}^L G$

if one can choose a representative $c^S \in \mathcal{C}_{\text{aut}}^S(G)$ of c such that

$$\text{ord}_{s=1}(L(s, c^S, r)) = [r : 1_{L_G}]$$

where $[r : 1_{L_G}]$ denotes the multiplicity of the trivial 1-dimensional representation of ${}^L G$ in r , and $L(s, c^S, r)$ is the L -function assumed to have meromorphic continuation for any representation r of ${}^L G$.

9.2. PRELIMINARIES

9.2.1. Tits System

Source: Humphreys Linear Algebraic Groups p 176, [41].

Let G be a group generated by subgroups B and N . Suppose $T = B \cap N$ is normal in N . Let $W = N/T$. Suppose that W is generated by a set S of involutions, i.e. elements of order 2. (G, B, N, S) is called a Tits system, if

(T1) If $\rho \in S$, $\sigma \in W$, then $\rho B \sigma \subset B \sigma B \cup B \rho \sigma B$

(T2) If $\rho \in S$, $\rho B \rho \neq B$.

W is called the Weyl group of the Tits system, and $\text{Card} S$ is the rank. B or any of its conjugates in G , is called a Borel subgroup of G .

9.2.2. Reductive Group, Quasisplit

Source: [17] Borel, “Linear Algebraic Groups”.

For an T endomorphism of a vector space V , T is nilpotent if $T^n = 0$, it is semisimple if its minimal polynomial has distinct roots (i.e. diagonalizable), and unipotent if $1 - T$ is nilpotent. In additive Jordan decomposition, one can write every endomorphism as a sum of a semisimple and nilpotent endomorphism: $T = T_s + T_n$. In the multiplicative form, one can write every endomorphism as a product of a semisimple and unipotent endomorphism $T = T_s T_u$. (Note $T_s + T_n = T_s(1 + T_s^{-1} T_n)$, and since T_s and T_n commute. So that $T_u = 1 + T_s^{-1} T_n$.)

Elements in an (affine) algebraic group G can also be decomposed into a semisimple and unipotent part. Here the notions of semisimple and unipotent carry over to algebraic groups by considering them as embedded inside $GL_n(k)$, as a closed subgroup.

The radical of an algebraic group G denoted by $R(G)$ is the greatest connected normal subgroup of G . The unipotent radical $R_u(G)$ is the greatest connected unipotent normal subgroup of G .

An algebraic group is said to be semisimple if $R(G) = \{e\}$ and reductive if $R_u(G) = \{e\}$.

See [41], p 223 for split and quasisplit groups. Also see [89] p 271.

A reductive group G is said to be k -split if G has a maximal torus which is k -split and an additional condition is satisfied.

It is said to be k -quasisplit if G has a Borel subgroup defined over k .

9.2.3. Theorem on Reductive Groups and Root Systems

In Borel's article "Automorphic L-functions" [14] there is the following statement:

There is a canonical bijection between isomorphism classes of connected reductive k -groups and isomorphism classes of root systems. It is defined by associating to G the root datum $\phi(G) = (X^*(T), \phi, X_*(T), \phi^v)$ where T is a maximal torus of G , $X^*(T)$ ($X_*(T)$) the group of characters (1-parameter subgroups) of T and Φ (Φ^v) the set of roots (coroots) of G with respect to T .

Further reference is given to Springer's article "Reductive Groups" [90].

9.2.4. Automorphic Representation

Suppose G is a connected reductive algebraic group over F , assumed for simplicity to be quasisplit.

An automorphic representation of G is an irreducible representation π of the adelic group $G(\mathbb{A})$ that is a constituent of the regular representation of $G(\mathbb{A})$ on $L^2(G(F) \backslash G(\mathbb{A}))$. Being a constituent is formally defined in Langlands' article "On the notion of an automorphic representation" [61].

9.2.5. L -group and L -homomorphism

These are defined in Borel's article "Automorphic L-Functions" [14].

Let E be a field and H, G connected reductive E -groups. A homomorphism $u : {}^L H \rightarrow {}^L G$ over Γ_k is said to be an L -homomorphism if it is continuous and if its restriction to ${}^L H^0$ is a complex analytic homomorphism of ${}^L H^0$ into ${}^L G^0$.

9.2.6. Automorphic Family and $\mathcal{C}_{\text{aut}}(G)$

9.2.7. Type A_0

Let $\pi = \otimes_{\nu} \pi_{\nu}$ be an automorphic representation of a reductive (quasisplit) group G over F .

Let $\phi_{\nu} : L_{F_{\nu}} = W_{F_{\nu}} \rightarrow {}^L G_{\nu}$ be an L -homomorphism attached to each archimedean component π_{ν} of π .

Suppose $G_{\text{der}} = [G, G]$ is simply connected. (G_{der} denotes derived subgroup, commutator subgroup.)

π is said to be of type A_0 if for every finite dimensional representation r of ${}^L G$ whose kernel contains a subgroup of finite index in W_F , the associated representations $r \circ \phi_{\nu}$ of archimedean Weil groups $W_{F_{\nu}}$ are of Hodge type, i.e. the restriction of $r \circ \phi_{\nu}$ to the subgroup $\mathbb{C}^*$ of $W_{F_{\nu}}$ is a direct sum of characters of the form

$$z \mapsto z^{-p} \bar{z}^{-q}, \quad z \in \mathbb{C}^*, \quad p, q \in \mathbb{Z}$$

An automorphic family $c \in \mathcal{C}_{\text{aut}}(G)$ is of the type A_0 if π is of type A_0 , for any automorphic representation π of G with $c(\pi) = c$. This subfamily will be denoted by $\mathcal{C}_{\text{aut},0}(G)$.

9.2.8. Weil-Taniyama Group

Taniyama group is an extension

$$1 \longrightarrow \mathcal{S}_F \longrightarrow \mathcal{T}_F \longrightarrow \Gamma_F \longrightarrow 1$$

of $\Gamma_F = \text{Gal}(\bar{F}/F)$ by the complex Serre group $\mathcal{S}_F$, a complex proalgebraic torus.

There is a natural transformation, as discussed in chapter 8, specifically theorem 25,

$$w \mapsto t(w), \quad w \in W_F$$

from W_F to $\mathcal{T}_F$ defined up to conjugation in $\mathcal{T}_F$ by its connected component $\mathcal{S}_F$, such that the following diagram commutes:

$$\begin{array}{ccccccc}
 & & & & W_F & & \\
 & & & \swarrow & \downarrow & & \\
 1 & \longrightarrow & \mathcal{S}_F & \longrightarrow & \mathcal{T}_F & \longrightarrow & \Gamma_F \longrightarrow 1
 \end{array}$$



10. COMPLEX MULTIPLICATION, ABELIAN VARIETIES AND PLECTIC

10.1. COMPLEX MULTIPLICATION

The following definition and result appears in [67] p 10.

Definition 176 • A number field E is said to be totally real if its image under every homomorphism $E \hookrightarrow \mathbb{C}$ is contained in $\mathbb{R}$.

- When the image is never contained in $\mathbb{R}$, the field is said to be totally imaginary.
- When one of the following three equivalent conditions is satisfied, the field is called a CM field:
 - E is a totally imaginary quadratic extension of a totally real number field
 - there exists a nontrivial automorphism ι_E of E such that $\rho \circ \iota_E = \iota \circ \rho$ for all (field) homomorphisms $\rho : E \hookrightarrow \mathbb{C}$
 - $E = F[\alpha]$ with F totally real and $\alpha^2 \in F$ and $\rho(\alpha^2) < 0$ for all homomorphisms $\rho : F \hookrightarrow \mathbb{C}$, where $\iota : \mathbb{C} \rightarrow \mathbb{C}$ is complex conjugation.

All quadratic extensions obtained by taking square root of a positive (squarefree) integer are totally real fields, whereas all quadratic extensions obtained by taking square root of a negative (squarefree) integer are totally imaginary. The cubic extension $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[x]/(x^3 - 2)$ is not totally real, since it can be embedded in $\mathbb{C}$ by the field homomorphism $x \mapsto \zeta_3 \sqrt[3]{2}$ where ζ_3 is primitive third root of unity. It is not totally imaginary either because $\mathbb{Q}[\sqrt[3]{2}]$ lies inside $\mathbb{R}$.

On the other hand $\mathbb{Q}[i, \sqrt{2}]$ is a totally imaginary quadratic extension of totally real number field $\mathbb{Q}[\sqrt{2}]$, hence is a CM field. Nontrivial automorphism of $\mathbb{Q}[i, \sqrt{2}]$ is given by $i \mapsto i^{-1} = -i$, which corresponds to complex conjugation of $\mathbb{C}$.

There is a notion of complex multiplication (type) of abelian varieties. This is described after defining abelian varieties in later sections of this chapter.

There are motives obtained from abelian varieties of CM type that have special properties. These are referred as CM motives, and they have a relation to Taniyama group. Below

results obtained about them by Deligne are described in the article "CM Motives and the Taniyama Group" by Schappacher [79] p 486-487:

"In Langlands's Märchen, the category of CM motives was hypothetical and the word 'motive' was not given a precise meaning. Soon after the Corvallis conference Deligne made progress on absolute Hodge cycles and the category of motives defined with them - see [Deligne 1979, 0,9-0.11], [20] cf. [Panchishkin 1993]. [75]

More precisely, Deligne was able to show that, on an abelian variety, every Hodge cycle is an absolute Hodge cycle: [Deligne (Milne), 1982]. [22] Thus, any category of motives for absolute Hodge cycles which is generated by a class of abelian varieties is not only well defined, but in it, we actually have at our disposal essentially all homomorphisms and objects that are expected to exist.

0.3.1. Using this manageable category of motives, Deligne was then able to prove, not later than the summer of 1981 [Deligne, 1982], [23] Langlands' Taniyama group is isomorphic to the motivic Galois group of the category $\mathcal{CM}_{\mathbb{Q}}$ of absolute Hodge cycle CM motives over $\mathbb{Q}$ (see 1 below for the precise definition of $\mathcal{CM}_{\mathbb{Q}}$). This theorem of Deligne solves the two problems mentioned in 0.1 above, to wit: (a) it generalizes the Shimura-Taniyama reciprocity law to all automorphisms of $\mathbb{C}$, and (b) it settles the problem about the L -function of a potentially CM abelian variety. See [Deligne, 1982, pp. 262/3: Remarques 4 and 2]. [23]."

In the following sections material building up to and including Dealing's result establishing isomorphism of Taniyama group to motivic Galois group of CM motives is described.

10.2. HODGE CYCLES AND MOTIVES

This section is a summary of the first four sections of the book [24], leading up to Deligne's result on motives and Taniyama group. It follows the introduction of this book, and the first four sections.

10.2.1. Hodge Cycles on Abelian Varieties

This subsection follows the introduction of [24] p 1-7 and the first section of the book which appears in references as [21].

Let X be a smooth projective variety over $\mathbb{C}$. Let X^{an} refer to the complex analytic manifold

associated to X . Considering projective embedding of X which defines a Kähler structure, the cohomology groups of X^{an} have a canonical decomposition $H^n = \bigoplus_{p+q=n} H^{p,q}$ called the Hodge decomposition. Cohomology class of an algebraic subvariety of codimension p is rational, i.e. is in $H^{2p}(X^{\text{an}}, \mathbb{Q})$, of bidegree (p, p) , i.e. lying in $H^{p,p}$. Hodge conjecture is the inverse of this statement, i.e.

Conjecture 6 (*Hodge Conjecture*) *Any element of $H^{2p}(X, \mathbb{Q}) \cap H^{p,p}$ is a linear combination over $\mathbb{Q}$ of the classes of algebraic subvarieties.*

Definition 177 *The rational (p, p) -classes are called Hodge cycles on X .*

Hodge conjecture asserts that rational (p, p) -classes, i.e. Hodge cycles are algebraic.

Definition 178 *A cohomology class $t \in H_{\text{DR}}^{2p}(X/k)$ is a Hodge cycle on X relative to $\sigma : k \hookrightarrow \mathbb{C}$ (a field embedding) if its image in $H^{2p}(X^{\text{an}}, \mathbb{C})$ is $(2\pi i)^p$ times a Hodge cycle on $X \otimes_{k, \sigma} \mathbb{C}$*

Theorem 26 (*Deligne*)

- *If X is an abelian variety then an element of $H_{\text{DR}}^{2p}(X/k)$ that is a Hodge cycle on X relative to one embedding of k in $\mathbb{C}$ is a Hodge cycle relative to all embeddings.*
- *For any embedding $(2\pi i)^p$ times a Hodge cycle in $H^{2p}(X^{\text{an}}, \mathbb{C})$ always lies in the image of $H_{\text{DR}}^{2p}(X/k)$.*

Due to this result, notion of being a Hodge cycle on an abelian variety is intrinsic to the variety (and independent of the embedding).

Note $H_{\text{DR}}^n(X/k) \otimes_{k, \sigma} \mathbb{C} \xrightarrow{\sim} H_{\text{DR}}^n(X^{\text{an}})$ is an isomorphism.

In fact, in the first article a stronger result is proved in which a Hodge cycle is defined to be an element of $H_{\text{DR}}^n(X) \times \prod H^n(X_{\text{et}}, \mathbb{Q}_l)$.

Deligne's proof utilizes parametrization of families of abelian varieties by Shimura varieties, and the notion of CM-type of an abelian variety.

10.2.2. Tannakian Categories

This subsection follows the introduction and the second section [22].

- In Tannakian categories, there are conditions that ensure that the category is equivalent to category of finite dimensional representations of an affine group scheme over a field.
- Category of polarizable $\mathbb{Q}$ -rational Hodge structures is Tannakian, and the group associated to its Tannakian subcategory of those Hodge structures of CM-type is called the connected Serre group S^0 . (Note this is called Serre group in this thesis).
- Motives (assuming standard conjectures) is Tannakian.
- Hodge motives (i.e. motives where algebraic cycles are replaced by Hodge cycles) on abelian varieties over a field is Tannakian.
- When motives are defined by abelian varieties over $\mathbb{C}$ of CM-type, the associated group is S^0 .
- When motives are defined by abelian varieties over $\mathbb{Q}$ that become of CM-type over $\mathbb{C}$, then the associated group is the Serre group S . (Note this is called Taniyama group $\mathfrak{T}$ in this thesis and in later articles.)

Here is a table of neutralized Tannakian categories C and the corresponding affine group scheme G such that this category is equivalent to the finite dimensional representations of that affine group scheme.

Category C	Affine Group Scheme G
Abelian varieties over $\mathbb{C}$ of CM type	S^0 , connected Serre group, Serre group
Abelian varieties over $\mathbb{Q}$ that become of CM type	Serre group S , Taniyama group $\mathfrak{T}$

Identity component of S is S^0

S is an extension of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by S^0

There is a continuous splitting $S(\mathbb{A}^f) \leftarrow \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$

Reason for the difference in naming Taniyama group is that these are defined differently by Deligne and are later shown to be isomorphic in a later section.

10.2.3. Langlands' Construction of Taniyama Group

Langlands' conjecture regarding Shimura varieties of abelian type is proved in later parts of the book .

Theorem 27 (Deligne) *Serre group together with its structure as an extension and its adelic splitting is isomorphic to Taniyama group*

The proof is a uniqueness argument of group extensions (extensions of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by S^0 with adèlic splittings) from properties of extensions. Group cohomology tells us when two extensions are isomorphic.

Significance of this result is the following: Taniyama group does not mention "abelian varieties of potential CM type", while Serre group does.

10.2.4. Motives and Taniyama Group

This section describes Deligne's result from his article [23].

Let T be Langlands' Taniyama group.

$$\begin{array}{ccccccc} 1 & \longrightarrow & T^0 & \longrightarrow & T & \longrightarrow & \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow 1 \\ & & \uparrow \mu & & & & \\ & & \mathbb{G}_m & & & & \end{array}$$

Here the system (T^0, μ) does not have nontrivial automorphisms, and this is the connected Serre group.

And there is a continuous section $T(\mathbb{A}^f) \xleftarrow{\pi} \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$

Note that the section is not a morphism of group schemes, and the continuous homomorphisms $\pi_l : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow T(\mathbb{Q}_l)$ induced from π have a Zariski-dense image. The system (T, π) does not have nontrivial automorphisms.

10.3. ABELIAN VARIETIES

This section and the following section reviews main definitions and known results of abelian varieties, polarization of an abelian variety and complex multiplication, following the following sources: [57], [87], [88].

Definition 179 *A divisor is an element of the free abelian group generated by all subvarieties of a variety of codimension one.*

Definition 180 *An abelian variety is a group variety which as a variety is complete.*

Topologically an abelian variety is a complex torus, that is for a discrete subgroup D of $\mathbb{C}^n$ of rank $2n$, $\mathbb{C}^n/D$.

Definition 181 *A homomorphism of an abelian variety A into an abelian variety B is a rational mapping λ such that $\lambda(x + y) = \lambda(x) + \lambda(y)$. If λ is birational then it is called an isomorphism.*

Lemma 121 *The homomorphisms from an abelian variety A into another abelian variety B , $\text{Hom}(A, B)$, is a finitely generated free $\mathbb{Z}$ -module.*

Notation: One sets $\text{Hom}_{\mathbb{Q}}(A, B) = \text{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$. Note then that the category of abelian varieties is a $\mathbb{Z}$ -linear category.

Theorem 28 *The group operation on an abelian variety is commutative.*

This follows by considering the dimension of the locus (x, yxy^{-1}) in $A \times A$ where A is an abelian variety.

Theorem 29 *Let A be an abelian variety and B an abelian subvariety of A . Then there exists an abelian subvariety C of A such that $A = B + C$, and $B \cap C$ is a finite group. If A and B are defined over a field k , then we can take C also defined over k .*

Definition 182 *For two abelian varieties A, B , A is isogeneous to B if there exists a surjective morphism $\lambda : A \rightarrow B$ whose kernel is finite.*

Remark: Shimura defines being isogeneous as:

Definition 183 *Two abelian varieties of the same dimension are isogeneous if there exists a homomorphism from one onto the other.*

Definition 184 *For $\lambda \in \text{Hom}(A, B)$, with A and B of same dimension, and k a field of definition of the abelian varieties, and x a generic point of A over k , and λ an isogeny,*

$$\nu(\lambda) = [k(x) : k(\lambda x)]$$

and

$$\nu_s(\lambda) = [k(x) : k(\lambda x)]_s, \quad \nu_i(\lambda) = [k(x) : k(\lambda x)]_i$$

and define ν, ν_s, ν_i as zero if λ is not an isogeny.

If λ is an isogeny, then $\nu_s(\lambda) = |\ker \lambda|$

Lemma 122 *The relation of isogeny is an equivalence relation.*

Definition 185 *An abelian variety is simple if its only abelian subvarieties are itself and zero.*

Theorem 30 *Every abelian variety is isogeneous to a product of simple abelian varieties, uniquely determined up to isogenies.*

Theorem 31 *The endomorphism ring of a simple abelian variety is a field.*

Theorem 32 *Let A be an abelian variety isogeneous to a product $\prod_{i=1}^m A_i^{n_i}$ of simple abelian varieties A_i mutually non-isogeneous. Let H_i be the complete ring of matrices of degree n_i over the field $\text{End}_{\mathbb{Q}}(A_i)$. Then $\text{End}_{\mathbb{Q}}(A)$ is isomorphic under the obvious natural mapping to the direct product of the rings H_i .*

Theorem 33 *Additive group of endomorphisms of an abelian variety is of finite type, and hence the algebra of endomorphisms is semi-simple.*

The last result follows by considering l -adic representations.

10.4. ABELIAN VARIETIES AND COMPLEX MULTIPLICATION

10.4.1. l -adic Representations of Homomorphisms

For an abelian variety A and a rational prime l , set

$$\mathfrak{g}_l(A) = \cup_{\alpha=1}^{\infty} \text{Ker}(l^{\alpha} 1_A)$$

Lemma 123 *If $\dim A = n$ and $l \neq \text{char } k$ where k is the field of definition of A , then $\mathfrak{g}_l(A) \cong \mathfrak{M} = (\mathbb{Q}_l/\mathbb{Z}_l)^{2n}$.*

Definition 186 *Any isomorphism of $\mathfrak{g}_l(A)$ onto $\mathfrak{M} = (\mathbb{Q}_l/\mathbb{Z}_l)^{2n}$ is called an l -adic coordinate system of $\mathfrak{g}_l(A)$.*

Lemma 124 *If $\mathfrak{o}$ and $\mathfrak{m}$ are l -adic coordinate systems of $\mathfrak{g}_l(A)$ and $\mathfrak{g}_l(B)$ where A and B are abelian varieties of dimension n and m respectively, and $\lambda : A \rightarrow B$ is a homomorphism of abelian varieties, then there exists $M \in M_{2m \times 2n}(\mathbb{Z}_l)$ such that*

$$\mathfrak{m}(\lambda t) = M \mathfrak{o}(t)$$

for $t \in \mathfrak{g}_l(A)$, and this correspondence $\lambda \mapsto M$ can be uniquely extended to a $\mathbb{Q}$ -linear map of $\text{Hom}_{\mathbb{Q}}(A, B)$ into $M_{2m \times 2n}(\mathbb{Q}_l)$.

Note the commutative diagram:

$$\begin{array}{ccccccc} A & \xleftarrow{\quad} & \mathfrak{g}_l(A) & \xrightarrow{\mathfrak{o}} & (\mathbb{Q}_l/\mathbb{Z}_l)^{2n} & \xleftarrow{\quad} & \mathbb{Q}_l^{2n} \\ \downarrow \lambda & & \downarrow & & \downarrow & & \downarrow M \in M_{2m \times 2n}(\mathbb{Z}_l) \\ B & \xleftarrow{\quad} & \mathfrak{g}_l(B) & \xrightarrow{\mathfrak{m}} & (\mathbb{Q}_l/\mathbb{Z}_l)^{2m} & \xleftarrow{\quad} & \mathbb{Q}_l^{2m} \end{array}$$

Definition 187 *The map defined in the lemma above is called an l -adic representation of $\text{Hom}_{\mathbb{Q}}(A, B)$ with respect to l -adic coordinate systems $\mathfrak{o}$ and $\mathfrak{m}$.*

10.4.2. Riemann Form

Definition 188 *Let D be a discrete subgroup of $\mathbb{C}^n$ of rank $2n$. An $\mathbb{R}$ -bilinear form $E(x, y)$ on $\mathbb{C}^n$ with values in $\mathbb{R}$ is called a Riemann form on $\mathbb{C}^n/D$ if it satisfies:*

(R1) $E(x, y)$ is an integer on $D \times D$.

(R2) $E(x, y) = -E(y, x)$

(R3) *The form $(x, y) \mapsto E(x, \sqrt{-1}y)$ is a positive (and not necessarily nondegenerate) symmetric form.*

A complex torus $\mathbb{C}^n/D$ has structure of an abelian variety if and only if there exists a non-degenerate Riemann form on $\mathbb{C}^n/D$ ([88] p 20).

10.4.3. Polarization of a Variety

Recall that a scheme X is regular in codimension one (or sometimes nonsingular in codimension one) if every local ring $\mathcal{O}_x$ of X of dimension one is regular ([39] p 130).

Let V be a complete variety, non-singular in co-dimension 1, defined over a field k .

For a divisor X on V which is rational over k , let $L(X; k)$ be the set of functions f on V defined over k such that $\text{div}(f) > -X$, where $\text{div}(f)$ is the divisor of the function.

$$L(X; k) = \{f : V \rightarrow k \mid f : \text{defined over } k, \text{div}(f) > -X\}$$

If k' is an extension of k , then $L(X; k') = L(X; k) \otimes_k k'$. Thus dimension of the vector space $L(X; k)$ over k (which is always finite) is independent of k . This is denoted by $l(X)$.

$$l(X) = \dim_k(L(X; k))$$

For a basis $\{f_0, \dots, f_r\}$ of $L(X; k)$ over k and x a generic point of V over k , consider $(f_0(x), \dots, f_r(x))$ as a point of the projective space $\mathbb{P}^r$ of dimension r and let U be the locus of $(f_0(x), \dots, f_r(x))$ over k .

Let $\Phi(x) = (f_0(x), \dots, f_r(x))$ be the rational mapping Φ of V onto U with respect to k .

Definition 189 *The divisor X is ample if the mapping Φ is biregular and $\{\text{div}(f) + X \mid f \in L(X; k)\}$ has no fixed component.*

Remark: The book [87] defines ample only by the mapping Φ being biregular and birational and does not mention the fixed component condition.

Lemma 125 *This definition is independent of choice of k and $\{f_i\}$ (basis of $L(X; k)$).*

Definition 190 *Let $\mathcal{C}(X)$ be the set of all divisors X' on V for which there exist two positive integers m, m' such that mX is algebraically equivalent to $m'X'$. The set $\mathcal{C}(X)$ is called a polarization of V if it contains an ample divisor. A variety V is polarizable if there exists a polarization of V . Polarized variety is a couple $(V, \mathcal{C})$. Elements of $\mathcal{C}$ are called polar divisors of $(V, \mathcal{C})$. $(V, \mathcal{C})$ is said to be defined over k if k is a field of definition for V and $\mathcal{C}$ contains a divisor rational over k .*

[57] p 193-194, [88] p 25, [87] p 26-27.

10.4.4. Picard Variety

The following result is from [88] p 5, [87] p 2-3. Picard variety of an abelian variety is treated in detail in [57] p 114-122.

Given an abelian variety A , let $\text{Div}_{\text{alg}}^0(A) = \mathcal{G}_a(A)$ and $\text{Div}_{\text{lin}}^0(A) = \mathcal{G}_l(A)$ denote the set of divisors on A algebraically equivalent to zero and the set of divisors on A linearly equivalent to zero.

Theorem 34 *There exists an abelian variety $\text{Pic}(A) = A^*$ canonically isomorphic to $\mathcal{G}_a(A)/\mathcal{G}_l(A)$. It is called the Picard variety of A .*

For a divisor $Y \in \mathcal{G}_a(A)$, let $\text{Cl}(Y)$ denote its class in $\text{Pic}(A) = A^*$.

Lemma 126 *Every homomorphism $\lambda : A \rightarrow B$ determines a homomorphism $\text{Pic}(\lambda) = \lambda^* : \text{Pic}(B) \rightarrow \text{Pic}(A)$ by*

$$\lambda^*(\text{Cl}(Y)) = \text{Cl}(\lambda^{-1}(Y))$$

whenever $\lambda^{-1}(Y)$ is defined. This mapping $\lambda \mapsto \lambda^*$ uniquely extends to an isomorphism of $\text{Hom}_{\mathbb{Q}}(A, B)$ onto $\text{Hom}_{\mathbb{Q}}(B^*, A^*)$, and ${}^t\alpha$ (transpose of α) denotes the image of α under this isomorphism.

For X a divisor on A let X_u denote the transform of X under translation by u $x \mapsto x + u$ on A .

Lemma 127 *Every divisor X of A defines a ϕ_X homomorphism of A into A^* by*

$$\phi_X(u) = \text{Cl}(X_u - X)$$

for $u \in A$.

Definition 191 *A divisor X is said to be non-degenerate if ϕ_X is an isogeny.*

Lemma 128 (Barsotti, Serre) *For two divisors X, Y in A $\phi_X = \phi_Y$ if and only if X and Y are algebraically equivalent.*

Lemma 129 *For a non-degenerate divisor X , and $\xi \in \text{End}_{\mathbb{Q}}(A)$, let*

$$\xi' = \phi_X^{-1} {}^t \xi \phi_X$$

Then $\xi \mapsto \xi'$ is an involution of $\text{End}_{\mathbb{Q}}(A)$. If a suitable multiple of X is ample, then for

every $\xi \neq 0$

$$\text{tr}(\xi\xi') > 0$$

Definition 192 *The involution of $\text{End}_{\mathbb{Q}}(A)$ of the previous lemma is called the involution of $\text{End}_{\mathbb{Q}}(A)$ determined by X .*

Lemma 130 *Let $\lambda \in \text{Hom}(A, B)$ and Y a divisor on B . If $\lambda^{-1}(Y)$ is defined, then for $X = \lambda^{-1}(Y)$, we have*

$$\phi_X = {}^t\lambda\phi_Y\lambda$$

10.4.5. Analytic Coordinate System of an Abelian Variety

Let A be an abelian variety defined over $\mathbb{C}$. Then there exists a complex torus $\mathbb{C}^n/D$ (with D being a discrete subgroup of rank $2n$) and an analytic isomorphism $\theta : A \rightarrow \mathbb{C}^n/D$. The pair $(\mathbb{C}^n/D, \theta)$ or θ is called an analytic coordinate system of A . If X is a divisor on A then $\theta(X)$ is an analytic divisor of $\mathbb{C}^n/D$.

10.4.6. Rational and Analytic Representations

Let A_1 and A_2 be two abelian varieties defined over $\mathbb{C}$ with analytic coordinate systems $(\mathbb{C}^n/D_1, \theta_1)$ and $(\mathbb{C}^n/D_2, \theta_2)$.

For a homomorphism $\lambda : A_1 \rightarrow A_2$, there exists a linear mapping $\Lambda : \mathbb{C}^n \rightarrow \mathbb{C}^m$ such that

$$\theta_2 \circ \lambda = \Lambda \circ \theta_1$$

and

$$\Lambda(D_1) \subset D_2$$

Conversely every linear mapping of $\mathbb{C}^n$ into $\mathbb{C}^m$ satisfying the latter condition, there exists a homomorphism of A_1 into A_2 .

Let $S = (s_{ij})$ be the $m \times n$ matrix with complex coefficients representing Λ with respect to coordinate systems (z_i) of $\mathbb{C}^n$ and (w_i) of $\mathbb{C}^m$.

Definition 193 *The mapping $\lambda \mapsto \Lambda$ (or $\lambda \mapsto S$), extended to $\text{Hom}_{\mathbb{Q}}(A_1, A_2)$ is called the analytic representation of $\text{Hom}_{\mathbb{Q}}(A_1, A_2)$ with respect to analytic coordinate systems θ_1 and*

θ_2 .

Let $\{u_1, \dots, u_{2n}\}$ and $\{v_1, \dots, v_{2m}\}$ be bases of D_1 and D_2 over $\mathbb{Z}$. Since Λ maps D_1 into D_2 , there exists a $2m \times 2n$ matrix $M = (r_{ij})$ with coefficients in $\mathbb{Z}$ such that

$$\Lambda(u_j) = \sum_{i=1}^{2m} r_{ij} v_i \quad (1 \leq j \leq 2n)$$

Definition 194 *The correspondence $\lambda \mapsto M$ can be uniquely extended to a representation of $\text{Hom}_{\mathbb{Q}}(A_1, A_2)$, and is called the rational representation of $\text{Hom}_{\mathbb{Q}}(A_1, A_2)$ with respect to $\{u_i\}$ and $\{v_i\}$.*

Lemma 131 *Rational representation of $\text{End}_{\mathbb{Q}}(A)$ is equivalent to l -adic representation.*

Lemma 132 *Rational representation of $\text{End}_{\mathbb{Q}}(A)$ is equivalent to the direct sum of the analytic representation and its complex conjugate.*

Letting U denote the $n \times 2n$ matrix whose column-vectors are $u_1, \dots, u_{2n}$ and V the $m \times 2m$ matrix whose column vectors are $v_1, \dots, v_{2m}$, we have

$$SU = VM$$

Letting $\bar{X}$ be the complex conjugate of a matrix, we have

$$\begin{pmatrix} S & 0 \\ 0 & \bar{S} \end{pmatrix} \begin{pmatrix} U \\ \bar{U} \end{pmatrix} = \begin{pmatrix} V \\ \bar{V} \end{pmatrix} M$$

When $A_1 = A_2$ and $n = m$ and $D_1 = D_2$ and $\theta_1 = \theta_2$ and $U = V$, the matrix $\begin{pmatrix} U \\ \bar{U} \end{pmatrix}$ is invertible.

10.4.7. CM-types

Let R be an algebra over $\mathbb{Q}$ with identity 1.

Definition 195 *An abelian variety of type (R) is a couple (A, ι) formed by an abelian variety A and an isomorphism ι of R into $\text{End}_{\mathbb{Q}}(A)$, such that $\iota(1) = 1_A$.*

Let F be an algebraic number field, and (A, ι) an abelian variety of type (F) and $n = \dim A$.

Lemma 133 $[F : \mathbb{Q}] = 2n$.

Lemma 134 Assume characteristic of F is zero and $[F : \mathbb{Q}] = 2n$, and M is a rational representation and S an analytic representation of $\text{End}_{\mathbb{Q}}(A)$, with respect to an analytic coordinate-system. Let $\phi_1, \dots, \phi_{2n}$ be all the isomorphisms of F into $\mathbb{C}$. Representation M restricted to F is equivalent to the direct sum of ϕ_i and S is equivalent to the direct sum of half of the $2n$ isomorphisms, say $\phi_1, \dots, \phi_n$ and $\bar{S}$ is equivalent to the direct sum of the remaining half, say $\phi_{n+1}, \dots, \phi_{2n}$. Hence no two isomorphisms among $\phi_1, \dots, \phi_n$ (or among the remaining n) are complex conjugate of each other. Furthermore F is totally imaginary (can not be embedded in the real numbers).

Definition 196 When the conditions of the above lemma hold, (A, ι) is said to be of type $(F, \{\phi_1, \dots, \phi_n\})$

Definition 197 For an algebraic number field F of degree $2n$ and n distinct isomorphisms ϕ_i of F into $\mathbb{C}$, (field homomorphisms), $(F; \{\phi_1, \dots, \phi_n\})$ is a CM-type if there exists an abelian variety of dimension n of type $(F; \{\phi_1, \dots, \phi_n\})$.

Remark: A field is totally real if all its embeddings inside $\mathbb{C}$ lie in $\mathbb{R}$. It is totally imaginary if no embedding inside $\mathbb{C}$ falls inside $\mathbb{R}$.

Theorem 35 In order that $(F; \{\phi_i\})$ to be a CM-type it is necessary and sufficient that F contains two subfield K and K_0 satisfying the following:

- (CM1) K_0 is totally real and K is a totally imaginary quadratic extension of K_0
- (CM2) There are no two isomorphisms among the ϕ_i which are complex conjugate of each other on K .

10.5. DELIGNE'S RESULT ON CM MOTIVES AND TANIYAMA GROUP

10.5.1. Motives

Source: Deligne's article [20], section on motives.

Definition 198 An additive category is Karoubian if all projectors (idempotent endomorphisms) are defined by a direct sum decomposition.

Lemma 135 *Each additive category has a Karoubian envelop, obtained by formally adjoining the images of projectors.*

Definition 199 *The category of effective motives over k is the Karoubian envelop of motives over k .*

Definition 200 *Tate motif $\mathbf{Z}(-1)$ is defined as direct factor $H^2(P^1)$ of $H^*(P^1)$.*

Lemma 136 (1) *Symmetry for commutativity of tensor product for Tate motif is identity.*

(2) *The functor $M \mapsto M \otimes \mathbf{Z}(-1)$ is fully faithful.*

10.5.2. Artin Motives

Definition 201 *Category of Artin motives is the Karoubian envelop of the dual of the category whose objects are varieties over $\mathbb{Q}$ of dimension zero, whose morphisms are correspondences defined over $\mathbb{Q}$.*

Each variety of dimension zero defines an Artin motif $H(X)$ and the functor H is contravariant and fully faithful. All Artin motives are a direct factor of such an $H(X)$.

10.5.3. CM Motives

Let F be a field of characteristic zero.

Let $(CM)_F$ denote the Tannakian category of motives over F generated by Artin motives (i.e. by zero cohomology of finite algebraic varieties) and by abelian varieties over F potentially of type CM (i.e. which become of CM type over an extension of F).

The category of motives $(CM)_{\mathbb{Q}}$ is equipped with a fiber functor H_B (rational cohomology over $\mathbb{C}$, and gives rise to a group M such that

- (1') A surjective morphism $M \rightarrow \Gamma_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ with kernel M^0 .
- (2') A morphism $\mu : \mathbb{G}_m \rightarrow M^0$ defined over $\mathbb{C}$, and the system (M^0, μ) does not have any nontrivial automorphisms.
- (3') A continuous section $\Gamma_{\mathbb{Q}} \rightarrow M(\mathbb{A}^f)$ of the surjective morphism in (1').

These parallel the conditions for Taniyama group as an extension of connected Serre group by Galois group.

The morphism (1') comes from the restriction of H_B to the category of Artin motives identified with rational representations of $\Gamma_{\mathbb{Q}}$.

To each representation V of M corresponds a motive V_1 and $V = H_B(V_1)$ and $V \otimes \mathbb{C}$ is equipped with a Hodge bigrading, and in particular an action μ of $\mathbb{G}_m$ given by

$$z * v^{p,q} = z^{-p} v^{p,q}$$

for $v^{p,q}$ being an element of $V \otimes \mathbb{C}$ of type (p, q) .

This action, being compatible with tensor product, provides a morphism μ defined over $\mathbb{C}$ of $\mathbb{G}_m$ in M . This is the structure in (2').

$V \otimes \mathbb{A}^f$ is the $\mathbb{A}^f$ -cohomology of V_1 and as such is equipped with an action of $\Gamma_{\mathbb{Q}}$. These actions provide (3').

Theorem 36 *Taniyama group T is isomorphic to $M = \text{Mot}(CM)$ (motivic Galois group of CM motives).*

Theorem is proved in a series of lemmas

In particular relation of CM motives to Hodge $\mathbb{Q}$ -structures of CM type is established. In particular equivalence of those two categories is established.

A $\mathbb{Q}$ -structure of Hodge is of CM type if it is polarizable and its Mumford-Tate group is abelian.

10.6. PLECTIC TANIYAMA GROUP

This section is based on [10].

Definition 202 *For a number field F , the group $\text{Aut}_F(F \otimes_{\mathbb{Q}} \bar{\mathbb{Q}})$ is called the F -plectic Galois group.*

Definition 203 *Plectic group is the following:*

$$\Gamma_{\mathbb{Q}} \sharp \Gamma_F = \{ \alpha : \Gamma_{\mathbb{Q}} \xrightarrow{\sim} \Gamma_{\mathbb{Q}} \mid \alpha(gh) = \alpha(g)h \text{ for } g \in \Gamma_{\mathbb{Q}}, h \in \Gamma_F \}$$

These two groups are canonically isomorphic.

In this article, the exact sequence defined for Serre-Taniyama groups is extended to the plectic setting to introduce an extension of the form:

$$1 \longrightarrow S_F \longrightarrow T_F \longrightarrow \mathrm{Aut}_F(F \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}) \longrightarrow 1$$

Classical theory is also reinterpreted in terms of Tate's half-transfer map. In particular the relations (embeddings) and exact sequences formed by taking how two field extensions of the same base field one containing the other are studied, to repeat Serre-Taniyama construction in a slightly different setting. In particular relation to complex multiplication fields is discussed.

11. MAIN RESULTS

11.1. GENERAL IDEAS

Langlands group should fit inside a commutative diagram.

$$WA_K \rightarrow L_K \rightarrow W_K \rightarrow G_K$$

These form commutative diagrams when the field K is replaced by another field that this field sits in, such that upon abelianization one obtains the exact sequence of abelian class field theory.

WA_K is isomorphic to a semidirect product. (consequence corollary 2.18 in Ikeda's paper [46])

There is also theorem 4.2 in [46] which says that Langlands group should fit to a commutative square.

$$\begin{array}{ccc} WA_K & \longrightarrow & L_K \\ \downarrow & & \downarrow \\ \mathcal{J}_K & \longrightarrow & W_K \end{array}$$

where $\mathcal{J}_K$ is the group that the Weil-Arthur idèle group projects onto.

It may be also necessary to consider the relative groups to obtain Langlands group more precisely.

If the map $WA_K \rightarrow W_K$ can be assumed as known, then the Langlands group should be the splitting of this map.

Here looking at [42], the nonabelian global reciprocity map (also known as the norm residue symbol) is a map from the group $\mathcal{J}_K$ into W_K this is theorem 1 in [42].

Hence the Langlands group should really fit inside, since the map above from WA_K into W_K should split through $\mathcal{J}_K$.

It is open that this homomorphism is open continuous and surjective.

To possibly attack continuity, one needs to identify generic open subsets of Weil group, which should have something to do with smaller Weil groups sitting inside a Weil group W_E inside W_K and take the preimage under norm-residue symbol, which is constructed to preserve "level sets" or "layers". The same argument can prove continuity. see for example corollary 1 on page 87 on [42]. For not being yet clear on the layers and topology on the Weil-Arthur idèle group, (it should be free product topology, possibly with Graev metric. Are the components locally compact topological groups? in which case the commutator should play a role.)

For surjectivity, one possible route to take is to consider the composition of the norm residue symbol with the map from Weil group to Galois group, and prove density there. It seems preferable since the Weil group is defined in class field theory, through these maps. However if one reconsiders the layers of the Weil group on page 13 [46], if one has a similar table for global nonabelian class field theory, then maybe one could try to find the layer of Weil group that the image sits in, and argue that if the map was not surjective, then Weil-Arthur idèle group could have been made larger or obtain a contradiction.

In order to pin down Langlands group, a direction is as follows, assuming that I am reading the papers correctly the question boils down to parametrizing groups that split a homomorphism.

Suppose $f : A \rightarrow C$ is a group homomorphism (if need be continuous) assuming surjectivity. Let's consider all possible splittings of this map to

$$A \xrightarrow{h} B \xrightarrow{g} C$$

Let's assume for simplification that h is surjective. (Otherwise B is something that contains the image of h and is larger, but the essential information of f is captured in the image of h , and the restriction of g on the image.) Assume that

$$f = g \circ h$$

then $\ker(h) \leq \ker(f)$, and $\ker(f)/\ker(h) \cong \ker(g)$. And furthermore $B \cong A/\ker(h)$ In other words we can parametrize all possible splittings of the homomorphism through normal

subgroups of $\ker(f)$

In other words B is constructed as A/N where $N \leq \ker(f)$ and normal.

Of course which of these groups is the correct one, and whether one can be found, needs to be checked against the formal properties of the Langlands group.

However it seems that the required conditions listed in on a group closely related, do not seem to indicate much other than that Langlands group will be a splitting of the nonabelian residue symbol from Weil Arthur idèle group into the Weil group. Maybe the other thing that needs to be checked is "representing the functor" mentioned in the beginning of the paper.

In Arthur's principle of functoriality, p 47 [7] there is an extension, and a candidate proposed as the Langlands group, from a fiber product. It seems that if this is the case, then the norm residue symbol is expected to factor through.

11.2. MAIN RESULTS – SKETCH

Maybe the following is a commutative diagram that holds:

$$\begin{array}{ccc}
 WA_F & \longrightarrow & \mathfrak{J}_F \\
 \downarrow & & \downarrow \\
 L_F & \longrightarrow & W_F \\
 \downarrow & & \downarrow \\
 \mathcal{G}_F & \longrightarrow & \mathfrak{I}_F \\
 \downarrow & & \downarrow \\
 \text{Mot}_F & \longrightarrow & \Gamma_F
 \end{array}$$

In the article "On a group closely related to the automorphic Langlands group " by K. I. Ikeda Theorem 4.2 [46] states that

$$\begin{array}{ccc}
 \mathcal{WA}_K & \longrightarrow & L_K \\
 \downarrow & & \downarrow \\
 \mathcal{J}_K & \longrightarrow & W_K
 \end{array}$$

is a commutative diagram, with horizontal arrows coming from norm-residue map (Langlands and Weil form). Here $\mathcal{WA}_K$ is the Weil-Arthur idèle group of the number field K . $\mathcal{J}_F$ is non-abelian idèle group. So the top square has been constructed in that article.

Arthur's article "Automorphic Langlands Group" [6] mentions two exact sequences:

$$1 \longrightarrow K_F \longrightarrow L_F \longrightarrow W_F \longrightarrow 1$$

and

$$1 \longrightarrow D_F \longrightarrow \mathcal{G}_F \longrightarrow \mathcal{T}_F \longrightarrow 1$$

And the construction of the second exact sequence is related to the map

$$t : W_F \rightarrow \mathcal{T}_F$$

Arthur's article principle of functoriality [7] that the construction of $\mathcal{G}_F$ and L_F parallel each other, hence there is a homomorphism

$$L_F \rightarrow \mathcal{G}_F$$

Furthermore if the homomorphism

$$L_F \rightarrow \mathcal{G}_F$$

does fit to a commutative diagram, since K_F sits injectively inside L_F and D_F sits injectively inside $\mathcal{G}_F$, if the homomorphism fits $t : W_F \rightarrow \mathcal{T}_F$ as mentioned then the following diagram is known:

$$\begin{array}{ccccccc} & & & & W A_F & \longrightarrow & \mathcal{J}_F \\ & & & & \downarrow & & \downarrow \\ 1 & \longrightarrow & K_F & \longrightarrow & L_F & \longrightarrow & W_F \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & D_F & \longrightarrow & \mathcal{G}_F & \longrightarrow & \mathcal{T}_F \longrightarrow 1 \\ & & & & & & \downarrow \\ & & & & & & \Gamma_F \end{array}$$

One question to ask is if we know the kernel of the homomorphism $W A_F \rightarrow \mathcal{J}_F$.

One other point is whether the two exact sequences do in fact form a commutative diagram.

Arthur's articles seem to suggest that this is the case.

The other problem is where to fit the motivic Galois group. Either $\mathcal{G}_F$ is the motivic Galois group, which Arthur says requires proof, or motivic Galois group comes with a projection to the full Galois group. In Serre's "Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques" [86] it is proved that if a collection of motives dominates (contains) another collection, then there is a surjective morphism from the motivic Galois group of the dominating collection to the motivic Galois group of the smaller collection. In particular this is so for Γ_F which is the motivic Galois group of the zero-dimensional motives. From Deligne's "Motifs et groupe de Taniyama" [23] it is also known that $\mathcal{T}_F$ the Taniyama group, is the motivic Galois group of CM motives. So for sure we know:

$$\begin{array}{ccc} & & \mathcal{T}_F \\ & \nearrow & \downarrow \\ \text{MotGal}_F & \longrightarrow & \Gamma_F \end{array}$$

Now what has been argued above is recapitulated into a theorem:

Theorem 37 • *There is a map from Weil-Arthur idele group into the Taniyama group, which is isomorphic to CM motives given as the composition:*

$$W A_F \longrightarrow \mathcal{I}_F \longrightarrow W_F \longrightarrow \mathcal{T}_F$$

where $W A_F$ is the Weil-Arthur idele group described in [46] and [42], $\mathcal{I}_F$ is the nonabelian idèle class group, described in the same papers, W_F is the Weil group, $\mathcal{T}_F$ is the Taniyama group.

- *The map above fits into a commutative diagram with the group $\mathcal{G}_F$ being the map constructed from fibre products in [6].*

$$\begin{array}{ccccccc} & & W A_F & \longrightarrow & \mathcal{J}_F & & \\ & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & K_F & \longrightarrow & L_F & \longrightarrow & W_F \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & D_F & \longrightarrow & \mathcal{G}_F & \longrightarrow & \mathcal{T}_F \longrightarrow 1 \\ & & & & & & \downarrow \\ & & & & & & \Gamma_F \end{array}$$

where L_F is the Langlands group, $K_F, D_F, \mathcal{G}_F$ are groups described both in previous chapters and in [6], [7].

It should be possible furthermore either to argue that $\mathcal{G}_F$ is indeed the motivic Galois group.

11.3. AUTOMORPHISM GROUP OF A FUNCTOR

The discussion below is written in the hope that what is argued below may be used in establishing the connection of motivic Galois group to $\mathcal{G}_F$, rigorously.

The natural equivalences from a functor $\mathcal{F} : \mathcal{C} \rightarrow \mathcal{D}$ to itself form a group.

If $\eta : \mathcal{F} \rightarrow \mathcal{F}$ is a natural equivalence from a functor to itself, this means that

- (i) For each object X in $\mathcal{C}$ we have morphisms $\eta_X : \mathcal{F}(X) \rightarrow \mathcal{F}(X)$ in $\text{Aut}_{\mathcal{D}}(\mathcal{F}(X)) \subset \text{Hom}_{\mathcal{D}}(\mathcal{F}(X), \mathcal{F}(X))$, and
- (ii) For each pair of objects X, Y of $\mathcal{C}$ and each morphism $f : X \rightarrow Y$ in $\text{Hom}_{\mathcal{C}}(X, Y)$, we have the commutative diagram

$$\begin{array}{ccc} \mathcal{F}(X) & \xrightarrow{\eta_X} & \mathcal{F}(X) \\ \mathcal{F}(f) \downarrow & & \downarrow \mathcal{F}(f) \\ \mathcal{F}(Y) & \xrightarrow{\eta_Y} & \mathcal{F}(Y) \end{array}$$

i.e.

$$\mathcal{F}(f) \circ \eta_X = \eta_Y \circ \mathcal{F}(f)$$

- (iii) Each η_X is an automorphism, i.e. an endomorphism that has an inverse.

- (iv) If ζ and η are two such natural equivalences, they can be composed to give a natural equivalence $\zeta \circ \eta$ where $(\zeta \circ \eta)_X = \zeta_X \circ \eta_X$ and $(\zeta \circ \eta)^{-1} = \eta^{-1} \circ \zeta^{-1}$.

- (v) The set of natural equivalences between $\mathcal{F}$ and itself is denoted by $\text{NatEq}(\mathcal{F}, \mathcal{F}) = \text{Aut}(\mathcal{F})$. By above this is a group.

- (vi) For each object X of $\mathcal{C}$, $\text{Aut}(\mathcal{F})(X)$, is a subgroup of $\text{Aut}_{\mathcal{D}}(\mathcal{F}(X))$, consisting of $\{\eta_X \mid \eta \in \text{Aut}(\mathcal{F})\}$

(vii) In other words we have projection morphisms

$$\mathrm{Aut}(\mathcal{F}) \rightarrow \mathrm{Aut}_{\mathbf{D}}(\mathcal{F}(X))$$

$$\eta \mapsto \eta_X$$

(viii) The projections “commute” with $\mathcal{F}(f)$ in the sense

$$\mathcal{F}(f) \circ \eta_X = \eta_Y \circ \mathcal{F}(f),$$

(ix) In particular, the image of the above projection in (vii), lies inside the centralizer of $\mathcal{F}(\mathrm{Aut}_{\mathbf{C}}(X))$ in $\mathrm{Aut}_{\mathbf{D}}(\mathcal{F}(X))$ (Seen simply by taking $Y = X$)

(x) Hence $\mathrm{Aut}(\mathcal{F})$ can be seen to lie inside

$$\prod_{X \in \mathrm{ob}(\mathbf{C})} C_{\mathrm{Aut}_{\mathbf{D}}(\mathcal{F}(X))}(\mathcal{F}(\mathrm{Aut}_{\mathbf{C}}(X))) \leq \prod_{X \in \mathrm{ob}(\mathbf{C})} \mathrm{Aut}_{\mathbf{D}}(\mathcal{F}(X))$$

(xi) Furthermore the compatibility relation can be expressed as:

$$\eta_Y^{-1} \circ \mathcal{F}(f) \circ \eta_X = \mathcal{F}(f)$$

for all $f \in \mathrm{Hom}_{\mathbf{C}}(X, Y)$

(xii) If we consider

$$\mathrm{Hom}_{\mathbf{C}} = \sqcup_{(a,b) \in \mathrm{ob}(\mathbf{C})^2} \mathrm{Hom}_{\mathbf{C}}(a, b)$$

with projection map

$$f \mapsto (\mathrm{source}(f), \mathrm{target}(f))$$

$$\mathrm{Hom}_{\mathbf{C}} \rightarrow \mathrm{ob}(\mathbf{C}) \times \mathrm{ob}(\mathbf{C})$$

then $\mathrm{Aut}(\mathbf{F})$ acts on sections of the projection map

$$\mathrm{Hom}_{\mathbf{D}} \rightarrow \mathrm{ob}(\mathbf{C}) \times \mathrm{ob}(\mathbf{C})$$

by

$$f_{a,b}^\eta = \eta_b^{-1} \circ f_{a,b} \circ \eta_a$$

where $f_{a,b}$ is the (a, b) –component of an element of a section f of the projection.

Under this terminology, it is required that we focus on those elements of $\prod_{X \in \text{ob}(\mathbf{C})} \text{Aut}_{\mathbf{D}}(\mathcal{F}(X))$ that act trivially on sections of $\mathcal{F}(\text{Hom}_{\mathbf{C}}) \leq \text{Hom}_{\mathbf{D}}$ under the projection to $\mathcal{F}(\text{ob}(\mathbf{C})) \times \mathcal{F}(\text{ob}(\mathbf{C})) \leq \text{ob}(\mathbf{D}) \times \text{ob}(\mathbf{D})$.

In other words

(xiii) The group

$$\prod_{X \in \text{ob}(\mathbf{C})} \text{Aut}_{\mathbf{D}}(\mathcal{F}(X))$$

acts on the “set” (whenever this is a set) of sections of

$$(\text{source}, \text{target}) : \text{Hom}_{\mathbf{D}} \rightarrow \text{ob}(\mathbf{D}) \times \text{ob}(\mathbf{D})$$

by

$$f_{a,b}^\eta = \eta_b^{-1} \circ f_{a,b} \circ \eta_a$$

where $f_{a,b}$ is the (a, b) –component of an element of a section f of the projection, and preserves fibers.

(That’s a fancy way of saying it acts on $\text{Hom}_{\mathbf{D}}(a, b)$ for all pairs (a, b) of objects of $\mathbf{D}$.)

The stabilizer of the set of sections of $\mathcal{F}(\text{Hom}_{\mathbf{C}}) \rightarrow \text{ob}(\mathbf{D}) \times \text{ob}(\mathbf{D})$ is $\text{Aut}(\mathcal{F})$.

(Alternatively stabilizer of $\mathcal{F}(\text{Hom}_{\mathbf{C}}(a, b))$ for all pairs (a, b) of objects of $\mathbf{C}$).

12. CONCLUSIONS

This is a review of the thesis.

Chapter 1, Category theory background reviews the terms of category theory relevant for this thesis.

Initial material is somewhat standard. Definition of subobject is carefully defined following Grothendieck's Tohoku paper.

Radical of a category, Semisimple categories are sketched and details are left to the sources.

Reason for discussing radical of a category is because there is a notion of semisimplicity in abstract algebra. Notion of semisimplicity for categories is an analogous notion, and requires being able to see a category as something that is like a ring, possessing ideals.

Fibered categories are defined.

Equivalence of category theoretic limit and colimit with projective and direct limits is carried out.

Chapter 2, Algebraic geometry reviews terms of algebraic geometry relevant for this thesis.

Definition of variety is discussed at the end. This term has slightly different meanings in different contexts, and the differences are pointed out.

Affine group scheme is only sketched.

Chapter 3, Tannakian categories defines tensor categories, up to tannakian categories.

Tensor category is defined. Then the constraint isomorphisms for tensor structure of a category is defined. These are associativity, commutativity and unit. Then there are compatibility of these constraints, in pairs.

The compatibility between associativity and commutativity constraint seems to be missing conditions. The rationale for why there is something missing is given, and this is discussed in the remark.

There is also the notion of a reduced unit as well as a unit constraint. If there is an associativity constraint, this determines a unit constraint from a reduced unit alone.

Compatibility of Assoc and Comm and Assoc Unit together imply compatibility of Commutativity and Unit.

Invertible object is defined,

Internal hom is defined.

Tensor functors, and their compatibility with constraints is defined.

Tensor equivalence is defined.

Rigid tensor category is defined.

Neutral tannakian category is defined (common to Saavedra and Deligne-Milne).

Then representations...

Here the idea is important, in that a group is to be reconstructed as group of tensor automorphisms...

A full discussion of the main theorems regarding tannakian categories is omitted because this relies on notion of gerbes.

But what is known as tannakian duality is important.

Important Remark In particular one of the main questions surrounds when/if the category of varieties, category of motives, and category of graded vector spaces which are also algebras is Tannakian, and if we can simply view the Motivic Galois group as the endomorphisms of cohomology ring, preserving grading...

Chapter 5, Motives and Motivic Galois Group

First there is the terminology of intersection theory, Notion of adequate equivalence relation, Weil cohomology theory.

Then there is the definition of category of motives.

What is known about the category of motives is not clear, because the morphisms are not understood... Serre's article remains a mystery...

Chapter 6, Standard Conjectures

Standard conjectures are stated in this section. Unfortunately there is not much of an interpretation, nor is the link to Weil conjectures explicitly stated, but only mentioned. These

are somewhat available in the sources. It would require a review of complex manifolds and Hodge theory and decomposition.

Chapter 7, Weil Group and Algebraic Number Theory

This chapter defines Weil group in algebraic number theory, and goes over Tate's Number Theoretic Background. Weil group comes from breaking down Artin Reciprocity map. Its construction relies on group cohomology, in particular second group cohomology which classifies group extensions. In particular, commutative diagrams involving relative Weil group are investigated.

Chapter 8, Serre-Taniyama Group

In Abelian l -adic representations, Serre gives a construction of Serre and Taniyama groups. The main theorem behind the construction is proved in detail. Algebraic tori are reviewed, as Serre group at field level can be seen as an algebraic torus. Langlands' construction of Serre-Taniyama group is investigated in detail through the viewpoint of group cohomology.

Chapter 9, Arthur's construction of Langlands Group

This chapter outlines Arthur's construction of Langlands group. Brief review of some terminology involved in the construction is carried out. The construction is outlined into the steps involving a fibre product.

Chapter 10, Complex Multiplication and Plectic

This chapter defines complex multiplication, abelian varieties, and quotes Deligne's results involving these objects. The most important result is that Taniyama group is isomorphic to the Motivic Galois group of certain motives called CM motives. There is also a small section on Plectic Taniyama group.

Chapter 11, Main Results

This chapter mentions the main result proved based on and assuming Arthur's construction of Langlands group. It states the commutative diagram involving Langlands group, Weil-Arthur idele group (which is defined in this section), Weil group, Taniyama group. Under the assumption that the motivic Galois group is isomorphic to the group in Arthur's construction, a stronger result could be asserted.

If one assumes that the standard conjectures are true, in particular that numerical and rational

equivalence are identical, then the motives constructed from numerical equivalence and rational equivalence would coincide.

According to Serre's article *Motifs* [85] p 339, assuming the standard conjectures, the category of motives, when the field is given an embedding into $\mathbb{C}$, is an abelian semisimple tannakian $\mathbb{Q}$ -category. In particular the details of the dependence that the motivic Galois group being a Tannakian category, on standard conjectures can be found in [48]. The importance of establishing that category of motives is Tannakian comes from a result which states that in Tannakian categories which is stated as proposition 3.11 on p 157 of [22]. When a tensor category is Tannakian, then an extension of the fibre functor defines an equivalence of tensor categories between the Tannakian category and the representations of the automorphism group of the functor. On p 130-131, theorem 2.11 [22] states conditions for automorphism group of an exact faithful tensor functor to be representable by an affine group scheme, and an equivalence of tensor categories. This condition is that the tensor category be rigid and abelian with endomorphism of the unit object being a field. There is also an intermediate result, theorem 3.2 on p 149 of [22] that holds for neutral tannakian categories regarding representability of tensor natural transformations between two fibre functors.

REFERENCES

1. Aluffi P. *Algebra*. AMS 2009.

2. André Y. Pour une théorie inconditionnelle des motifs. *Publications mathématiques de l'I.H.É.S.* tome 83. 1996:5-49

Available from: http://www.numdam.org/item?id=PMIHES_1996__83__5_0

3. André Y, Kahn B. Construction inconditionnelle de groupes de Galois motiviques, *Comptes Rendus Mathématique, C. R. Acad. Sci. Paris.* Ser. I vol 334. 2002: 989-994.

4. André Yves, Kahn B. Nilpotence, radicaux et structures monoïdales. (avec un appendice de Peter O'Sullivan) *Rendiconti del Seminario Matematico della Università di Padova*, University of Padua / European Mathematical Society. Tome 108. 2002:107-291.

Available from: <https://arxiv.org/pdf/math/0203273.pdf> and from http://www.numdam.org/item/RSMUP_2002__108__107_0/

5. André Y. *Introduction Aux Motifs (Motifs Purs, Motifs Mixtes, Périodes) Panoramas et Synthèses [Panoramas and Syntheses]* vol 17. Société Mathématique de France, 2004.

6. Arthur J. A Note on the Automorphic Langlands Group. *Canad. Math. Bull.* Vol. 45 (4), 2002:466-482

7. Arthur J. The principle of functoriality. *Bulletin (New Series) of the American Mathematical Society*. Volume 40, Number 1. (electronically published in) 2002:39-53.

8. Artin M, Grothendieck A, Verdier JL. (with collaborators: Bourbaki N, Deligne P, Saint-Donat B.) *Séminaire de Géométrie Algébrique du Bois Marie 1963-64 Théorie des topos et cohomologie étale des schémas*(SGA 4) TOME 1: Theorie des Topos (Exposés I à IV) Springer-Verlag, 1972.
9. Bénéabou J. Des Catégories Fibrées, *Lecture Notes by J.-R. Roisin of a Course by J. Bénéabou at Univ. Louvain-la-Neuve* (1980)
10. Blake C. A plectic Taniyama group.2016. Available from: <https://arxiv.org/pdf/1606.03320v1.pdf>
11. Bourbaki N. *Algebre*. Hermann, Paris, 1958.
12. Bourbaki N. *Théorie des ensembles*. Hermann, Paris, 1970.
13. Bourbaki, N. Univers. *SGA 4* 1972: 185-217.
14. Borel A. Automorphic L-functions. Appears in *Proceedings of Symposia in Pure Mathematics*. Vol. 33 part 2. 1979:27-61.
15. Borel A. Groupes Linéaires Algébriques. *Annals of Mathematics*. 64(1), 1956:20-82.
16. Borel A. *Linear algebraic groups*. Springer-Verlag, New York, 1991.
17. Borel A. Linear Algebraic Groups. Appears in *Algebraic Groups and Discontinuous Subgroups, Proceedings of Symposia in Pure Mathematics*. (Borel A, Mostow GD. editors) v 9. 1966:3-19.
18. Cassels J W S, Fröhlich A. *Algebraic Number Theory: Proceedings of an instructional conference organized by the London Mathematical Society*. Academic Press,1967.

19. Chevalley C. - Deux théorèmes d'arithmétique. *J. Math. Soc. Japan*, 3. 1951:36-44.
20. Deligne P. Valeurs de fonctions L et périodes d'intégrales. *Automorphic Forms, Representations, and L-Functions. Proc. Sympos. Pure Math.* vol. XXXIII, part 2. Amer. Math. Soc, Providence, RI, 1979:313-346.
21. Deligne P. (Notes by Milne JS.) Hodge cycles on abelian varieties. Appears in *Hodge Cycles, Motives and Shimura Varieties*. Editors: Deligne P, Milne J. S. , Ogus A. , and Shih K. *Lecture Notes in Math.*, vol. 900. Springer-Verlag, Berlin and New York. 1982:9-100.
22. Deligne P, Milne J. S. Tannakian categories. *Hodge Cycles, Motives and Shimura Varieties*. Editors: Deligne P., Milne J. S. , Ogus A. , and Shih K. *Lecture Notes in Math.*, vol. 900. Springer-Verlag, Berlin and New York. 1982:101-228.
23. Deligne P. Motifs et groupe de Taniyama. *Hodge Cycles, Motives and Shimura Varieties*. Editors: Deligne P, Milne JS, Ogus A, Shih K. *Lecture Notes in Math.*, vol. 900, Springer-Verlag. Berlin and New York, 1982:261-279.
24. Deligne P, Milne J, Ogus A, Shih K. *Hodge cycles, motives and Shimura varieties, Lecture Notes in Math.*, vol. 900, Springer-Verlag, Berlin and New York. 1982.
25. Demazure M. *Motifs des variétés algébriques*. Séminaire N. Bourbaki, 1971, exp. no 365, 1971:19-38. Available from: http://www.numdam.org/item?id=SB_1969-1970__12__19_0
26. Dummit D S, Foote R M. *Abstract Algebra*. John Wiley and Sons, Inc. 2004.
27. Eilenberg S, MacLane S. *General Theory of Natural Equivalences*. Transactions of the American Mathematical Society, Vol. 58, No. 2 Sep., 1945:231-294.
Available from <https://www.jstor.org/stable/1990284>

28. Freyd P. *Abelian Categories: An Introduction to the Theory of Functors*. Harper International September 1968.
29. Fulton W. *Intersection Theory*. Springer, 1998.
30. Gabriel P. Des catégories abéliennes. *Bull. Soc. Math. France*. 90, 1962:323-448.
31. Giraud J. *Cohomologie non abélienne*. Springer-Verlag 1971.
32. Griffiths P, Harris J. *Principles of Algebraic Geometry*. John Wiley & Sons, 1994.
33. Grothendieck A. Sur quelques points d'algèbre homologique. *Tohoku Math. J.* (2) Volume 9, Number 2. 1957: 119-221.
34. Grothendieck A. Généralités sur les groupes algébriques affines: Groupes algébriques affines commutatifs. *Séminaire Claude Chevalley*, tome 1 (1956-1958), exp. no 4. p. 1-14 which appears in *Séminaire C. Chevalley, Classification des groupes de Lie algébriques*, Ecole Norm. Sup. (Paris), 1958. Available from http://www.numdam.org/item?id=SCC_1956-1958__1__A4_0
35. Grothendieck A. Standard conjectures on algebraic cycles. *Algebraic Geometry* (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968) Oxford University Press, 1968:193-199 Available from <https://webusers.imj-prg.fr/~leila.schneps/grothendieckcircle/StandardConjs.pdf>
36. Grothendieck A. SGA I expose VI *Séminaire de Géométrie Algébrique du Bois Marie 1960-1961. Revêtements étales et groupe fondamental.(SGA 1)* Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud. *Lecture Notes in Mathematics*. Vol. 224. Springer-Verlag, Berlin-New York, 1971.
37. Artin M, Grothendieck A, Verdier JL. (with collaborators: Bourbaki N, Deligne P

Saint-Donat B.) *Séminaire de Géométrie Algébrique du Bois Marie 1963-64 Théorie des topos et cohomologie étale des schémas*(SGA 4) TOME 1: Theorie des Topos (Exposés I á IV) Springer-Verlag, 1972.

38. Grothendieck A, Verdier JL. Univers. *SGA 4*. Springer-Verlag, 1972: 1-4.
39. Hartshorne R. *Algebraic Geometry*. Springer-Verlag, 1977.
40. Hungerford T W. *Algebra*. Springer-Verlag 1974.
41. Humphreys J E. *Linear Algebraic Groups*. Springer 1975.
42. Ikeda, K. I. Basic Properties of the Non-Abelian Global Reciprocity Map. *Mathematics in the 21st Century. 6th World Conference, Lahore, March 2013*, ed.s Cartier Pierre, Choudary ADR, Waldschmidt Michel. Springer Proceedings in Mathematics & Statistics Volume 98. 2013:45-92.
43. Ikeda K. I. On the non-abelian global class field theory. *Annales mathématiques du Québec* 37(2). 2013:129-172.
44. Ikeda KI, Nair S, Süer E. *p-sel sayılar*. Çakılları Matematik Köyü, 2017. Available from: https://www.cakilarasimatematikkoyu.com/uploads/7/2/0/8/72089201/ders_notlari_p-sel_sayilar.pdf
45. Ikeda KI, Özlem S. *Weil Sanıları*. Çakılları Matematik Köyü, 2018. Available from: https://www.cakilarasimatematikkoyu.com/uploads/7/2/0/8/72089201/weilsanilaricakilarasi_prefinal.pdf
46. Ikeda K. I. On a group closely related with the automorphic Langlands group. *J. Korean Math. Soc. vol.57, no. 1* 2020: 21-59.

47. Jacobson N. *Basic Algebra*. H, W. H. Freeman & Co., San Francisco, 1980.
48. Jannsen U. Motives, numerical equivalence, and semi-simplicity. *Invent. math.* 107. 1992: 447-452.
49. Kelly G M. Complete functors in homology I. Chain maps and endomorphisms. *Proc. Camb. Phil. Soc.* 60. 1964:721-735.
50. Kelly G M. On Mac Lane's conditions for coherence of natural associativities, commutativities, etc. *Journal of Algebra* 4, 1964:397-402.
51. Kelly, G M. On the radical of a category. *J. Austral. Math. Soc.* 4. 1964:299-307.
52. Kelly G M, Mac Lane S. Coherence in closed categories. *Journal of Pure and Applied Algebra* 1. 1, 1971:97-140.
53. Kleiman S L. Algebraic cycles and the Weil conjectures. *Dix exposés sur la cohomologie des schémas*. Giraud, J. (ed.), Amsterdam: North-Holland, 1968:359-386.
54. Kleiman S L. Motives. *5th Nordic Summer-School in Mathematics, Oslo August 5-25, 1970, algebraic geometry*. Oort, F. (ed.), Oslo 1970. Groningen. 1972:53-82.
55. Kleiman S L. The Standard Conjectures. *Proceedings of the Summer Research Conference on Motives, held at the University of Washington, Seattle, Washington, July 20-August 2, 1991*. 1991:3-20.
56. Kottwitz R E. Rational conjugacy classes in reductive groups. *Duke Math. J.* 49(4)(December 1982): 785-806.
57. Lang S. *Abelian Varieties*. Springer-Verlag, 1983.

58. Lang S. *Algebraic Number Theory*. Springer-Verlag, 1994.
59. Lang S. *Algebra*. Springer-Verlag, 2002.
60. Langlands R P. Automorphic Representations, Shimura Varieties, and Motives. Ein Märchen. *Proceedings of Symposia in Pure Mathematics*. Vol. 33 part 2. 1979:205-246.
61. Langlands R P. On the notion of an automorphic representation. *Automorphic Forms, Representations and L-functions, Proc. Sympos. Pure Math.* Vol. 33, part 1, Amer. Math. Soc., 1979:203-207.
62. Langlands R P. Stable Conjugacy: Definitions and Lemmas. *Canadian Journal of Mathematics* Volume 31 , Issue 4 , 01 August 1979 , pp. 700 - 725
63. Leduc P Y. Catégories semi-simples et catégories primitives. *Canad, J. Math.* 20. 1968:612-628.
64. Mac Lane S. *Natural associativity and commutativity*. Rice University Studies 49. 1963:28-46.
65. Mac Lane S. *Categories for the working mathematician*. Springer-Verlag. 1998, 1971.
66. Milne J, Shih K.y. Langlands' construction of the Taniyama group. *Hodge Cycles, Motives and Shimura Varieties. Lecture Notes in Math.*, vol. 900, Springer-Verlag. (P. Deligne, J. S. Milne, A. Ogus, and K. Shih, eds.) Berlin and New York. 1982:229-260.
67. Milne JS. *Complex Multiplication*. 2006,2020. Available from: <https://www.jmilne.org/math/CourseNotes/CM.pdf>
68. Mitchell B. *Theory of Categories*. Academic Press, 1965.

69. Mitchell B. Rings with Several Objects. *Advances in Mathematics*. 8. 1972:1-161.
70. Nair S. *2-Trace Formulas on Finite Groups*. PhD Thesis, Yeditepe University, 2020.
71. Nekovar J. Hidden symmetries in the theory of complex multiplication. *Algebra, arithmetic, and geometry: in honor of Yu. I. Manin*. Vol. II., Progr. Math., 270. Birkhuser Boston, Inc., Boston, MA, 2009:399-437.
72. Nekovar J, Scholl A J. Introduction to plectic cohomology. *Advances in the theory of automorphic forms and their L-functions : workshop in honor of James Cogdells 60th birthday, October 16-25, 2013, Erwin Schrodinger Institute, University of Vienna, Vienna, Austria*. Editors: Jiang Dihua , Shahidi Freydoon , Soudry David. *Contemporary Mathematics* 664. AMS, 2016: 321-338.
73. Olsson M. *Algebraic Spaces and Stacks*. AMS Colloquium Publications 62, 2016.
74. Ono T. Arithmetic of Algebraic Tori. *Annals of Mathematics* , Jul., 1961, Second Series, Vol. 74, No. 1, Jul., 1961:101-139.
75. Panchishkin A A. Motives for absolute Hodge cycles, *Proceedings of Symposia in Pure Mathematics Volume 55, Motives*. Editors: Jannsen Uwe, Kleiman Steven, Serre Jean-Pierre. vol. 1, 1994: 461-483.
76. Ramakrishnan D, Valenza RJ. *Fourier Analysis on Number Fields*. Springer-Verlag, 1999.
77. Russell B. *The Principles of Mathematics*. (1st edition 1903). W. W. Norton & Company, Inc. 1938.
78. Saavedra R N. *Catégories Tannakiennes*. Lect. Notes in Math.265, Springer-Verlag 1972.

79. Schappacher Norbert. CM Motives and the Taniyama Group. *Proceedings of the summer research conference on motives held at the University of Washington Seattle, Washington, July 20-AUGUST 2, 1991*. 1991:485-508.
80. Serre, J.-P. Analogues Kähleriennes des certaines conjectures de Weil. *Annals of Mathematics* 71. 1960: 392-394.
81. Serre J-P. *Corps Locaux*. Publications de l'Institut de Mathématique de l'Université de Nancago, VIII, Actualités Sci. Indust., No. 1296. Hermann, Paris, 1962.
82. Serre J-P. Sur les groupes de congruence des variétés abéliennes. *Izv. Akad. Nauk. S.S.S.R.*, 28. 1964:3-20.
83. Serre J-P. *Algèbre Locale - Multiplicités*. (rédigé par P. Gabriel) Lecture Notes in Math. 11, Springer-Verlag, Heidelberg, 1965.
84. Serre J-P. *Abelian L-adic representations and elliptic curves*. Addison-Wesley, 1968, 1989.
85. Serre J-P. Motifs. *Astérisque*. Tome 198-199-200, 1991:333-349. Available from: http://www.numdam.org/item?id=AST_1991__198-199-200__333_0
86. Serre J-P. Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques. *Proceedings of Symposia in Pure Mathematics Volume 55 Part 1, Motives: Summer Research Conference on Motives (1991)* AMS, 1994: 377-400.
87. Shimura G, Taniyama Y. *Complex Multiplication of Abelian Varieties and its applications to number theory*. The Mathematical Society of Japan, 1961.

88. Shimura G. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1998.
89. Springer TA. *Linear algebraic groups*. 2nd ed. Birkhäuser, 1998.
90. Springer TA. Reductive Groups. Appears in *Proceedings of Symposia in Pure Mathematics* Vol. 33 part I, 1979: 3-27.
91. Street R. Ideals, radicals and structure of additive categories, *Appl. Cat. Structures* 3. 1995:139-149.
92. Streicher T. FIBRED CATEGORIES à la Jean Bénabou. preprint. 2018-2020. Available from: <https://arxiv.org/abs/1801.02927>
93. Tate J, Artin E. *Class Field Theory*. W. A. Benjamin, 1967.
94. Tate J. Number Theoretic Background. appears in *Proceedings of Symposia in Pure Mathematics Vol 33 Part 2, Automorphic Forms, Representations, and L-functions*. Borel, A. Casselman, W. (eds). 1979:3-26.
95. Waterhouse, W.C. *Introduction to affine group schemes*. Springer-Verlag, 1979.
96. Weil A. Sur la théorie du corps de classes. *J. Math . Soc. Japan* 3. 1951: 1 -35.
97. Weil A. *Adeles and Algebraic Groups*. Birkhäuser, 1982.
98. Weil A. *Variétés Kähleriennes*. Hermann, Paris, 1968.