Arithmetic for quantum circuits

Jon Yard

Edition 0.95

Contents

Introduction

We give a concise development of the mathematics underlying the theory of arithmetic groups towards applications in quantum computing, quantum information theory and quantum field theory. Rather than aim for pedagogy, we organize concepts from most general to least, so this is more like an instruction manual than a textbook. We begin with general preliminaries on monoidal categories, duality, abelian categories and tensor categories and continue with generalities on noncommutative rings with involution. A rapid introduction to schemes and commutative rings follows. We then describe the theory of separable algebras over fields with involution, specializing further to semisimple, simple, central simple and quaternion. Then we focus on integrality and discuss lattices and orders over integral domains and integral quadratic forms. We try not to avoid the prime 2 because bits and qubits are too important.

Later chapters develop local/global principles, Clifford algebras and superalgebras with involution. Future (hopefully near-final) revisions will better incorporate this material earlier while including more on affine algebraic groups, class numbers, Galois and class field theory.

Sources include

- *Maximal Orders* by Reiner [1]
- `https://stacks.math.columbia.edu/`
- *The Book of Involutions* [2]
- Lam, *A First Course on Noncommutative Rings* [3]
- Clark's lecture notes
  `http://alpha.math.uga.edu/~pete/noncommutativealgebra.pdf`
- J. W. S. Cassels - *Rational Quadratic forms* [4]
- Knus, *Quadratic and Hermitian Forms over Rings* [5]
- Scharlau, *Quadratic and Hermitian forms* [6]
- Gille and Szamuely, *Central Simple Algebras and Galois Cohomology* [7]
- Roquette, *The Brauer-Hasse-Noether Theorem: A Historical Perspective* [8]
- McConnell and Robson, *Noncommutative Noetherian Rings* [9]
- Nebe, Rains and Sloane *Self-dual codes and invariant theory* [10]
- Brown and Goodearl, *Lectures on Algebraic Quantum Groups*
- Pierce, *Associative Algebras*
- De Meyer and Ingraham, *Central Separable Algebras*

Chapter 0
Category theory

0.1 Basic definitions

0.1.1 Categories

A **category** C consists of a collection C_0 of **objects** and a collection C_1 of **morphisms**. Each morphism $f \in \mathsf{C}_1$ has a well-defined **source** $s(f) \in \mathsf{C}_0$ and **target** $t(f) \in \mathsf{C}_0$. We write $f : a \to b$ to mean that $s(f) = a$ and $t(f) = b$ and write $\mathrm{Hom}_{\mathsf{C}}(a, b)$ for the morphisms from a to b. Furthermore,

- If $f : a \to b$ and $g : b \to c$ are morphisms, their **composition** $gf : a \to c$ is a morphism.
- Composition is associative $h(gf) = (hg)f$.
- For each object a, there is an **identity morphism** $1_a : a \to a$ acting as the identity for left and right composition.

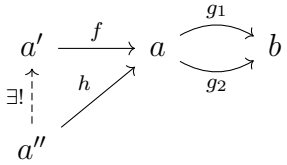
Examples: Set, Mon, Ab, Grp, Ring, R-mod, $\mathsf{Open}(X)$, $\mathsf{Path}(\mathsf{Q})$

We write $a = b$ for the proposition that a and b, however constructed, are equal, and may interpret it as a type whose elements are proof of such equality. A morphism $f : a \to b$ is an **isomorphism** if there exists a morphism $g : b \to a$ with $gf = 1_a$ and $fg = 1_b$. A category is **skeletal** if isomorphism implies equality, i.e. if it has a single object per **isomorphism class**.

0.1.2 Morphisms

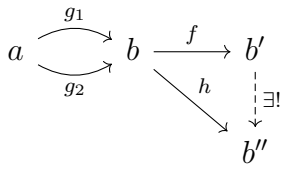
A morphism f is a **monomorphism**, or is **monic**, if it is left cancellable in the sense that $fg_1 = fg_2$ implies $g_1 = g_2$. A **subobject** of a is an equivalence class of monomorphisms $f : a' \to a$ under isomorphisms on a'. Reversing arrows, a morphism f is an **epimorphism**, or is **epic**, if it is right cancellable in the sense that $g_1 f = g_2 f$ implies $g_1 = g_2$, i.e. it only equalizes equal morphisms. A **quotient** of b is an equivalence class of epimorphisms $f : b \to b'$ under isomorphisms on b'.

A morphism f **equalizes** a pair g_1, g_2 of parallel morphisms if $g_1 f = g_2 f$. An **equalizer** of g_1 and g_2 is a morphism $f : a' \to a$ through which any other equalizing morphism $h : a' \to a$ factors uniquely



When they exist, equalizers are unique up to isomorphism so the corresponding subobject is called *the* **equalizer**. The uniqueness property implies that every equalizer is monic.

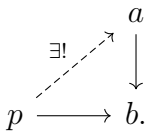
Similarly, f **coequalizes** parallel morphisms g_1 and g_2 if $fg_1f = fg_2$. A **coequalizer** is a morphism $f : b \to b'$ through which each coequalizing morphism $h : b \to b''$ factors uniquely



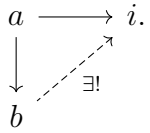
Similar to the case with equalizers, when coequalizers exist, they are are epic and unique up to isomorphism.

0.1.3 Objects

An object p is **projective** if each morphism $p \to b$ has a unique lift to any given epimorphism $a \to b$ as



Similarly, an object i is **injective** if each morphism $a \to i$ uniquely factors through each monomorphism $a \to b$ as in



An object is **Noetherian** if every increasing chain of subobjects (equivalently, decreasing chain of quotients) stabilizes, and **Artinian** if every decreasing chain of subobjects (equivalently, increasing chain of quotients) stabilizes.

An object is **initial** if it has a unique morphism to each object and **final**, or **terminal**, if it has a unique morphism from each object. A **zero object** is both initial and final. Such objects if they exist, are unique up to isomorphism. Example: $\mathbb{Z}$ and 0 are respectively the initial and final objects in Ring, wheres 0 is the zero object in any category of modules.

An object in a category with a zero object is **simple** if has exactly two nonzero subobjects (equivalently, quotients): the zero object and itself. An object is **finite** if it has a **composition series**, i.e. a finite sequence of successive subobjects with simple quotients. Finite objects are both Noetherian and Artinian. The **length** of a finite object is the length of any of its composition series.

0.1.4 Functors

Let C and D be categories. A **functor** $F\colon \mathsf{C} \to \mathsf{D}$ is an operation taking objects of C to objects of D and morphisms of C to morphisms of D, that is **covariant** in the sense that $F(f \circ g) = F(f) \circ F(g)$, $F(\mathrm{id}_x) = \mathrm{id}_{F(x)}$. A **contravariant functor** is defined similarly except that it reverses arrows: $F(f \circ g) = F(g) \circ F(f)$. A contravariant functor is the same thing as a covariant functor to the opposite category C^{op}.

0.1.5 Natural transformations

A **natural transformation** $\eta\colon F \to G$ between functors $F, G\colon \mathsf{C} \to \mathsf{D}$ is given by a **natural family** $\eta_x \in \mathrm{Hom}_{\mathsf{C}}(F(x), G(x))$ of morphisms such that for every morphism $f \in \mathrm{Hom}_{\mathsf{C}}(x, y)$ in C, we have $\eta_y F(f) = G(f)\eta_x$, i.e. the following diagram commutes:

$$\begin{array}{ccc} F(x) & \xrightarrow{F(f)} & F(y) \\ \downarrow{\scriptstyle \eta_x} & & \downarrow{\scriptstyle \eta_y} \\ G(x) & \xrightarrow{G(f)} & G(y). \end{array}$$

The **functor category** D^{C} is the category whose objects are functors from C to D and whose morphisms are natural transformations between them. **Subfuctors** are subobjects in functor categories.

An **equivalence** between C and D consists of a pair of mutually **quasi-inverse** functors $F : \mathsf{C} \to \mathsf{D}$ and $G : \mathsf{D} \to \mathsf{C}$, by definition equipped with natural isomorphisms $GF \simeq \mathrm{id}_{\mathsf{C}}$ and $FG \simeq \mathrm{id}_{\mathsf{D}}$ to the identity functors. A **duality** between the categories C and D is similarly given by a pair of contravariant functors satisfying the same condition.

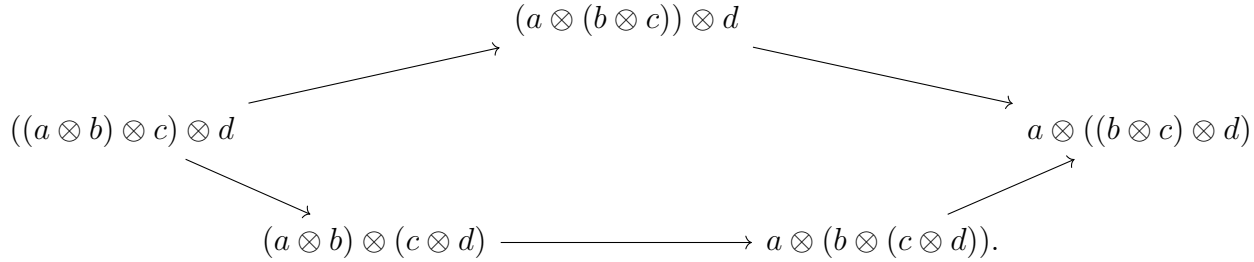
A **skeleton** of a category is an equivalent skeletal category.

Diagrams, products and coproducts.

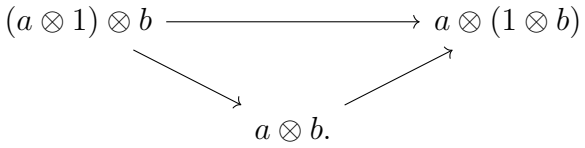
0.2 Monoidal categories

0.2.1 Coherence

A **monoidal category** is a category M equipped with a bifunctor $\otimes : \mathsf{M} \times \mathsf{M} \to \mathsf{M}$, a tensor unit $1_{\mathsf{M}} \in \mathsf{M}$, isomorphisms $1_{\mathsf{M}} \otimes 1_{\mathsf{M}} \to 1_{\mathsf{M}}$, $- \otimes 1_{\mathsf{M}} \to \mathrm{id}_{\mathsf{M}}$ and natural isomorphisms $1_{\mathsf{M}} \otimes - \to \mathrm{id}_{\mathsf{M}}$ and $(- \otimes -) \otimes - \to - \otimes (- \otimes -)$, the latter of which satisfies the pentagon equations



The unit isomorphisms define isomorphisms $1_{\mathcal{M}} \otimes a \to a$ and $a \otimes 1_{\mathcal{M}} \to a$ satisfying the triangle equations



Equivalently, the natural isomorphisms to id_{M} in the above definition can be replaced with isomorphisms $1_{\mathsf{M}} \otimes a \to a$ and $a \otimes 1_{\mathsf{M}} \to a$ satisfying the triangle equations.

A **monoidal functor** is a functor $F : \mathsf{M} \to \mathsf{N}$ between monoidal categories that is equipped with two **coherence morphisms**, $F(\cdot) \otimes_{\mathsf{N}} F(\cdot) \to F(\cdot \otimes_{\mathsf{M}} \cdot)$ (between functors $\mathsf{M} \times \mathsf{M} \to \mathsf{N}$) and $1_{\mathsf{N}} \to F(1_{\mathsf{M}})$, satisfying hexagon and square equations. The monoidal functor is **strict** if the coherence maps are equalities and **strong** if they are invertible. See Section 2.4 of [11] for more details.

There are $\frac{1}{n+1}\binom{2n}{n}$ ways of parenthesizing $x_1 \otimes \cdots \otimes x_n$. MacLane's Strictness Theorem ([11] 2.8.5) (each monoidal category is monoidally equivalent to a strict one) $\Rightarrow$ Coherence Theorem ([11] 2.9.2) (any two isomorphisms built from associativity and unit maps between parenthesizations of $x_1 \otimes \cdots \otimes x_n$ are equal).

0.2.2 Braidings and symmetry

A **braiding** on a monoidal category M is an endomorphism $R \in \mathrm{End}_{\mathsf{M}}(\otimes)$ of the tensor product functor $\otimes : \mathsf{M} \times \mathsf{M} \to \mathsf{M}$ satisfying

$$\begin{array}{ccc} a \otimes b & \xrightarrow{f \otimes g} & a' \otimes b' \\ \downarrow{\scriptstyle R_{a,b}} & & \downarrow{\scriptstyle R_{b',a'}} \\ b \otimes a & \xrightarrow{f' \otimes g'} & b' \otimes a' \end{array}$$

for all morphisms $f : a \to a'$ and $g : b \to b'$ as well as hexagon equations

$$\begin{array}{ccccc} & & (b \otimes a) \otimes c & \xrightarrow{F_{bac}} & b \otimes (a \otimes c) & & \\ & \nearrow{\scriptstyle R_{a,b}} & & & & \searrow{\scriptstyle R_{a,c}} & \\ (a \otimes b) \otimes c & & & & & & b \otimes (c \otimes a) \\ & \searrow{\scriptstyle F_{abc}} & & & & \nearrow{\scriptstyle F_{bca}} & \\ & & a \otimes (b \otimes c) & \xrightarrow{R_{a,b \otimes c}} & (b \otimes c) \otimes a & & \end{array}$$

for all triples a, b, c, along with identical equations for R^{-1}. A braiding R is **symmetric** if $R^2 = \mathrm{id}_M$.

The Drinfeld center $\mathsf{Z}_1(\mathsf{M})$ of any monoidal category M is braided.

0.2.3 Duals and traces

A **left dual** of an object x in a monoidal category consists of an object x^*, an **evaluation** morphism $\mathrm{ev}_x : x^* \otimes x \to 1$ and a **coevaluation** morphism $1 \to x \otimes x^*$ such that the following compositions are equal to the identity (suppressing the unit morphisms of M):

$$x \xrightarrow{\mathrm{coev}_x \otimes \mathrm{id}_x} (x \otimes x^*) \otimes x \xrightarrow{\alpha_{x,x^*,x}} x \otimes (x^* \otimes x) \xrightarrow{\mathrm{id}_x \otimes \mathrm{ev}_x} x$$

$$x^* \xrightarrow{\mathrm{id}_{x^*} \otimes \mathrm{coev}_{x^*}} x^* \otimes (x \otimes x^*) \xrightarrow{\alpha_{x^*,x,x^*}} (x^* \otimes x) \otimes x^* \xrightarrow{\mathrm{ev}_{x^*} \otimes \mathrm{id}_{x^*}} x^*.$$

A **right dual** to x is an object ${}^*x$ together with evaluation $\mathrm{ev}'_x \colon x \otimes {}^*x \to 1$ and coevaluation $\mathrm{coev}'_x \colon 1 \to {}^*x \otimes x$ morphisms such that the analogous compositions are identity morphisms:

$$x \xrightarrow{\mathrm{id}_x \otimes \mathrm{coev}'_x} x \otimes ({}^*x \otimes x) \xrightarrow{\alpha^{-1}_{x,{}^*x,x}} (x \otimes {}^*x) \otimes x \xrightarrow{ev'_x \otimes \mathrm{id}_x} x$$

$${}^*x \xrightarrow{\mathrm{coev}'_{{}^*x} \otimes \mathrm{id}_{{}^*x}} ({}^*x \otimes x) \otimes {}^*x \xrightarrow{\alpha^{-1}_{{}^*x,x,{}^*x}} {}^*x \otimes (x \otimes {}^*x) \xrightarrow{\mathrm{ev}_{{}^*x} \otimes \mathrm{id}_{{}^*x}} {}^*x.$$

When they exist, left or right duals are unique up to unique isomorphism.

A morphism $f : x \to y$ between objects with left duals gives a morphism $f^* : y^* \to x^*$ between their left duals and similarly for right duals if they exist.

An object x with left and right duals is called **dualizable** (or **rigid**) and satisfies ${}^*(x^*) \simeq x \simeq ({}^*x)^*$. A monoidal category is **rigid** if all of its objects are dualizable. Left/right duals on a rigid category extend to a pair of mutually quasi-inverse duality functors.

Exercise 2.10.15 in [11] explains the name: The only morphisms of monoidal functors between rigid categories are isomorphisms.

The evaluation and coevaluation morphisms define a left and a right **categorical trace**

$$\mathrm{Tr}_L : \mathrm{Hom}(x, x^{**}) \to \mathrm{End}(1), \quad \mathrm{Tr}_R : \mathrm{Hom}(x, {}^{**}x) \to \mathrm{End}(1)$$

for each rigid object x. If $x \simeq x^{**}$, then $\mathrm{Tr_L}(f)\,\mathrm{Tr_R}(f^{-1}) = \mathrm{Tr_R}(f)\,\mathrm{Tr_L}(f^{-1})$ takes the same value for every isomorphism $f : x \to x^{**}$ and therefore assigns a unique **squared dimension** $|x|^2 \in \mathrm{End}(1)$ to x. A rigid object is **invertible** if evaluation and coevaluation are isomorphisms, which is the case iff its squared dimension is 1.

A rigid monoidal category M is **pivotal** if it comes equipped with a **pivotal structure** $\mathrm{id}_{\mathsf{M}} \simeq **$. Composing with the constituent isomorphisms $x \to x^{**}$ defines a left and right **pivotal trace** $\mathrm{PTr_L}, \mathrm{PTr_R} : \mathrm{End}(x) \to \mathrm{End}(1)$ and **pivotal dimension** $\mathrm{Pdim_L}(x) = \mathrm{PTr_L}(1_x)$, $\mathrm{Pdim_R}(x) = \mathrm{PTr_R}(1_x)$ for each object x. If these dimensions coincide for all objects, then M is **spherical** and the pivotal dimension is $\mathrm{Pdim}(x) := \mathrm{PTr}(1_x)$. Note that spherical $\subset$ pivotal $\subset$ rigid.

0.2.4 Twists

Let B be a rigid braided category. The **Drinfeld isomorphism** ([11] Definition 8.9.4) on B is the natural isomorphism $u : \mathrm{id}_{\mathsf{B}} \to **$ defined by the compositions

$$a \to a \otimes a^* \otimes a^{**} \to a^* \otimes a \otimes a^{**} \to a^{**}.$$

For a proof that it is an isomorphism see Proposition 8.10.6 of [11]. It behaves as

$$u_a \otimes u_b = u_{a\otimes b} R_{ba} R_{ab}$$

under tensor products ([11] Proposition 8.9.3). The Drinfeld isomorphism u is a pivotal structure iff it is monoidal iff the braiding is symmetric. However, because every natural isomorphism $\mathrm{id}_{\mathsf{B}} \simeq **$ has the form $u\theta$ for some $\theta \in \mathrm{Aut}(\mathrm{id}_{\mathsf{B}})$ the twisted Drinfeld isomorphism $u\theta$ is a pivotal structure iff

$$\theta_{a\otimes b} = (\theta_a \otimes \theta_b) R_{ba} R_{ab}, \tag{1}$$

in which case θ is called a **twist** in Definition 8.10.1 of [11].

0.3 Enriched categories

Let M be a monoidal category. An **M-category**, or **category enriched** in M, is a category C in which each $\mathrm{Hom}_{\mathsf{C}}(a, b)$ is an object of M and each morphism of C corresponds to a morphism $1_{\mathcal{M}} \to \mathrm{Hom}_{\mathsf{C}}(a, b)$ in M, such that for each triple $a, b, c \in \mathsf{C}$ of objects, there is an associated morphism

$$\circ_{abc} : \mathrm{Hom}(b, c) \otimes \mathrm{Hom}(a, b) \to \mathrm{Hom}(a, c)$$

in M such that $\circ_{abc}(g \otimes f) = gf$ for all $f \in \mathrm{Hom}(a, b)$ and $g \in \mathrm{Hom}(b, c)$, subject to pentagon and triangle equations for associativity and units.

Example 0.3.1 A Set-category is called **locally small**.

Example 0.3.2 If R is a commutative ring, we call an R-mod-category an **R-linear category**.

Example 0.3.3 A Cat-category is called a **strict 2-category**, with monoidal structure given by the product of categories.

0.3.1 Locally small categories

A category C is **locally small** if it is a Set-category, so each $\mathrm{Hom}_{\mathsf{C}}(x, y)$ is a set. Such categories are always **well powered** (its subobjects form a set) and **well copowered** (its quotients form a set).

A functor $F\colon \mathsf{C} \to \mathsf{D}$ between locally small categories is an equivalence if it is **fully faithful** (i.e. each $\mathrm{Hom}_{\mathsf{C}}(x,y) \to \mathrm{Hom}_{\mathsf{D}}(F(x),F(y))$ is bijective) and **essentially surjective** (i.e. if every object of D is isomorphic to some $F(x)$ with $x \in \mathsf{C}$), in which case the rest of the required data can be shown to exist but is not uniquely specified by F.

A category is **small** if it is locally small and has a set of objects. A small category C is therefore described by a set C_0 of objects, a set C_1 of morphisms and four functions: $\mathsf{C}_1 \to \mathsf{C}_0$ (source and target objects of a morphism), $\mathsf{C}_1 \times_{\mathsf{C}_0} \mathsf{C}_1 \to \mathsf{C}_1$ (composition), $\mathsf{C}_0 \to \mathsf{C}_1$ (identity morphism). More generally, categories can be viewed as instantiations of abstract data types C_0 and C_1 with source, target, composition and identity being operations defined on these types.

A category is **essentially small** if it has a small skeleton, i.e. is equivalent to a small category, so its equivalence classes of objects form a set.

An essentially small category is **Noetherian/Artinian** if each object is, and if it has a zero object, it is **finite** if every object is.

Let C be a locally small category. If w is an object of C, then $\mathrm{Hom}(w,-) : \mathsf{C} \to \mathrm{Set}$ is a covariant functor taking each morphism $f : x \to y$ to the function $\mathrm{Hom}(w,f) : \mathrm{Hom}(w,x) \to \mathrm{Hom}(w,y)$. Similarly, for each object z, $\mathrm{Hom}(-,z) : \mathsf{C} \to \mathrm{Set}$ is a contravariant functor taking morphism $f : x \to y$ to the function $\mathrm{Hom}(f,z) : \mathrm{Hom}(y,z) \to \mathrm{Hom}(x,z)$. The contravariant Hom functor $\mathrm{Hom}(-,z) : \mathsf{C} \to \mathsf{Set}$ is also known as the **functor of points**.

0.3.2 Representable functors

A functor $F\colon \mathsf{C} \to \mathsf{Set}$ is **representable** if $F \simeq \mathrm{Hom}(x,-)$ for some object $x \in \mathsf{C}$. We say that x **represents** F. Each morphism $f \in \mathrm{Hom}(y,x)$ determines a natural transformation $\eta(f)\colon \mathrm{Hom}(x,-) \to \mathrm{Hom}(y,-)$ of functors whose components $\eta(f)_z\colon \mathrm{Hom}(x,z) \to \mathrm{Hom}(y,z)$ are right composition $\eta(f)_z(g) = g \circ f$ for $g \in \mathrm{Hom}(x,z)$.

Yoneda's Lemma shows that representations are unique up to unique isomorphism:

Lemma 0.3.1 (Yoneda's Lemma) Let C be a locally small category and let $F, G\colon \mathsf{C} \to \mathsf{Set}$ be functors represented by isomorphisms $\alpha\colon F \to \mathrm{Hom}(x,-)$ and $\beta\colon G \to \mathrm{Hom}(y,-)$. Then if $\gamma\colon F \to G$ is a morphism, there exists a unique $f \in \mathrm{Hom}(y,x)$ such that

$$\begin{array}{ccc} F(z) & \xrightarrow{\gamma_z} & G(z) \\ \downarrow{\scriptstyle \alpha_z} & & \downarrow{\scriptstyle \beta_z} \\ \mathrm{Hom}(x,z) & \xrightarrow{\eta(f)_z} & \mathrm{Hom}(y,z) \end{array}$$

commutes for each object $z \in \mathsf{C}$ and the the natural family $\gamma_z\colon F(z) \to G(z)$ acts as $\gamma_z = \beta_z^{-1} \circ \eta(f)_z \circ \alpha_z$.

A category C is **concrete** if it is equipped with a faithful functor $F : \mathsf{C} \to \mathsf{Set}$, and **concretizable** if such a faithful functor exists. Concrete categories formalize the notion of categories that are "realized by sets."

Exercise 0.3.1 Show that the category hTop of topological spaces and homotopy classes of maps between them is not concretizable.

Exercise 0.3.2 Show that every surjection in a concrete category is an epimorphism.

Concrete categories can contain non-surjective epimorphisms, such as $\mathbb{Z} \hookrightarrow \mathbb{Q}$ in Ring and $\mathbb{N} \hookrightarrow \mathbb{Z}$ in Mon. A morphism in the category of Hausdorff spaces and continuous maps is epic iff it has a dense image. On the other hand, every epimorphism is surjective in the categories of e.g. sets, posets, relations, groups, abelian groups, finite groups, modules, topological spaces and compact Hausdorff spaces.

Exercise 0.3.3 Show that an object p is projective iff the functor $\mathrm{Hom}(p, -)$ preserves epimorphisms. Characterize injective objects similarly using the functor of points.

Exercise 0.3.4 Show that the following are equivalent [12]:

- every set is projective
- the Axiom of Choice
- Zorn's Lemma
- the Well-ordering Theorem
- Tychonoff's Theorem: Products of compact spaces are compact for the product topology.

0.3.3 Preadditive categories

A **preadditive category** is an Ab-category, or equivalently, a $\mathbb{Z}$-linear category. It is a theorem that every finite product in a preadditive category is a coproduct and vice-versa, hence called a **biproduct** $\oplus$ or **sum** (direct or indirect, they are isomorphic and we will try not to worry about this in these notes).

Each object a of a preadditive category has an **endomorphism ring**

$$\mathrm{End}(a) = \mathrm{Hom}(a, a)$$

with multiplication given by composition. In particular, a preadditive category with

one object is a ring, just as a category with one object is a monoid and a groupoid with one object is a group.

The **kernel** of a morphism $f : a \to b$ in a preadditive category is defined to be the equalizer

$$\ker(f) \longrightarrow a \underset{0}{\overset{f}{\rightrightarrows}} b$$

of f and the zero morphism $0 : a \to b$. Similarly, the **cokernel** is the coequalizer

$$a \underset{0}{\overset{f}{\rightrightarrows}} b \longrightarrow \operatorname{coker}(f)$$

When they exist, they are unique up to isomorphism, as with all universal constructions. Kernels are are monic and cokernels are epic. The equalizer and coequalizer of f and g are $\ker(f-g)$ and $\operatorname{coker}(f-g)$.

If C and D are categories and D is preadditive, the functor category D^{C} is also preadditive. A functor $F : \mathsf{C} \to \mathsf{D}$ between preadditive categories is **additive** if, for each $a, b \in \mathsf{C}$, $F : \operatorname{Hom}(a,b) \to \operatorname{Hom}(F(a), F(b))$ is a homomorphism of abelian groups. If both C and D are preadditive, the **module category** $\mathsf{M}(\mathsf{C},\mathsf{D}) \subset \mathsf{D}^{\mathsf{C}}$ of additive functors and natural transformations between them is preadditive. To see that this generalizes the category of modules over a ring, note that if $\eta : F \to G$ is a morphism in $\mathsf{M}(\mathsf{C},\mathsf{Ab})$ and $a \in \mathsf{C}$, then $\eta_a : F(a) \to G(a)$ is a homomorphism of $\operatorname{End}(a)$-modules.

If R is a commutative ring, we call an R-mod-category a **linear category**, or an **R-linear category**. While some authors (e.g. [11]) further assume linear categories to be additive and over a field, we do not.

0.3.4 Additive categories

An **additive category** is a preadditive category with all biproducts. This includes the empty biproduct = the zero object, so there is a notion of simple object as one with no nontrivial subobjects. Non-simple objects in additive categories are **reducible** and the simple objects are **irreducible**. An object a in an additive category is **decomposable** if it has a decomposition $a = a_1 \oplus a_2$ for objects a_1 and a_2. Otherwise a is **indecomposable**. Simple implies indecomposable and therefore decomposable implies reducible. However, there can be reducible indecomposables whose subobject is not a summand, such as the representation $x \mapsto \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ of $\mathbb{R}$. Verma modules and quantum groups at roots of unity give further examples.

An object in an additive category is **semisimple** if it is a finite sum of simple objects. An essentially small additive category with semisimple objects is called **semisimple**. Note that semisimple $\Rightarrow$ finite $\Rightarrow$ Noetherian and Artinian.

The main example of an additive category is the category of projective modules over a ring. Other examples include the category of finitely generated modules over a non-Noetherian ring and the category of free modules over a commutative ring.

0.3.5 Exact categories and their Grothendieck rings

An **exact category** is an additive category with a class of distinguished short exact sequences $0 \to a \xrightarrow{m} b \xrightarrow{e} c \to 0$, containing all split sequences and closed under isomorphism. The morphisms in these sequences, **admissible monics** m and **admissible epis** e, must by definition satisfy the following requirements: If $b \to c$ is an admissible epi and $b' \to c$ is any morphism, there is an admissible epi from the **pullback** $b \times_c b' \to b'$. If $a \to b$ is an admissible monic and $a \to b'$ is any other morphism, there is an admissible monic to the **pushout** $a \to b +_a b'$. If the composition $a \to a' \to b$ is an admissible epi and $a \to a'$ has a kernel, then $a' \to b$ is an admissible ep. If $b \to c \to c'$ is an admissible monic and $c \to c'$ has a cokernel, then $b \to c$ is an admissible monic.

Every abelian category is exact. The **Grothendieck group** $K_0(\mathsf{C})$ of an essentially small exact category C is the abelian group generated by the isomorphism classes $[a]$ of simple objects subject to the relations $[b] = [a] + [c]$ for every exact $a \to b \to c$. For any ring A, the category of finitely generated projective A-modules is exact. Its Grothendieck group is denoted $K_0(A)$.

A functor between exact categories is **exact** if it is additive and maps exact sequences to exact sequences. A bifunctor $\otimes : \mathsf{C} \times \mathsf{C} \to \mathsf{C}$ is **exact** if the functors $- \otimes x$ and $x \otimes -$ are exact for every object $x \in \mathsf{C}$. Every essentially small monoidal category M with exact $\otimes$ has a **Grothendieck ring** $K_0(\mathsf{M})$.

If M is rigid, left and right duals define the same involution on $K_0(\mathsf{M})$. If M is pivotal, the quantum traces induce ring homomorphisms $K_0(\mathsf{M}) \to \mathrm{End}(1)$ that are exchanged by the involution and which coincide if M is spherical.

0.3.6 Preabelian categories

A **preabelian category** is an additive category with all kernels and cokernels. Each morphism f in a preabelian category therefore has a well-defined **image** $\mathrm{im}(f) = \ker(\mathrm{coker}(f))$ and **coimage** $\mathrm{coim}(f) = \mathrm{coker}(\ker(f))$, factoring as

$$a \to \mathrm{coim}(f) \to \mathrm{im}(f) \to b.$$

A functor between preabelian categories is **left exact** if it is additive and preserves kernels, **right exact** if it is additive and preserves cokernels and **exact** if it preserves both, hence exact sequences.

Examples of preabelian categories include

- The category of Hausdorff topological abelian groups: The image $\mathrm{im}(f)$ of a morphism $f : a \to b$ is the inclusion $\overline{f(a)} \hookrightarrow b$ of the the closure of the range of a, so that $f(a)$ is dense in $\mathrm{im}(f)$.
- The category of filtered modules over a ring A. It is R-linear when A is an R-algebra.

0.3.7 Abelian categories

We have seen that kernels are always monic and cokernels are always epic. The converse statements hold in abelian categories: A monomorphism is **normal** if it is a kernel and an epimorphism is **normal** if it is a cokernel. A preabelian category is **abelian** if every monomorphism and epimorphism is normal.

Each object in an abelian category has a composition series consisting of a sequence of subobjects with simple quotients.

Examples of abelian categories include

- The category of all modules over a ring.
- The category of finitely generated modules over a left-Noetherian ring.
- The category of compact Hausdorff spaces.
- The category of projective modules over a hereditary ring.

The **Freyd-Mitchell Theorem** states that every abelian category is equivalent to a full subcategory of some A-mod.

The ring homomorphism $\mathbb{Z} \to \mathbb{Q}$ is epic but not a cokernel, so for example its presence can keep a preabelian category from being abelian. For instance, this implies the category Ring is not abelian, but it also not even preadditive because it has no coproduct.

Nonexamples: The category of Hausdorff topological abelian groups is not abelian because morphisms with non-closed range are not normal. The category of filtered A-modules is preabelian but not abelian.

> **Exercise 0.3.5** Show that an abelian R-linear category is Artinian iff its homsets are finitely generated R-modules and its objects have finite length, and is finite iff it is equivalent to the category of finitely generated modules over a finitely generated R-algebra A.

Given a field k, [11] calls a k-linear abelian category **finite** if it is equivalent to the category of finite-dimensional modules over some finite-dimensional k-algebra A. Finite linear categories depend on A only up to Morita equivalence and are equivalently characterized as locally finite with finitely many isomorphism classes of simple objects such that each simple object has a projective cover.

0.4 Tensor categories

0.4.1 Multiring categories

We follow Sections 4.2-4.3 of [11] and define a **multiring category** over a commutative ring R to be an abelian Artinian monoidal category with biadditive and biexact tensor product.

The unit object 1_{R} of a multiring category R decomposes as a sum

$$1_{\mathsf{R}} \simeq \bigoplus_i 1_{\mathsf{R}_i}$$

of non-isomorphic indecomposables. A **ring category** is a multiring category with indecomposable unit.

The endomorphism ring $\mathrm{End}(1_{\mathsf{R}})$ of the unit 1_{R} in a multiring category R is a semisimple commutative algebra over the base ring. Over an algebraically closed field (the focus of [11]) this is just a direct product of copies of the field but more generally it will be a direct product of commutative ring extensions.

The components of the unit decompose R into subcategories

$$\mathsf{R}_{i,j} = 1_{\mathsf{R}_i} \otimes \mathsf{R} \otimes 1_{\mathsf{R}_j}$$

whose indecomposables partition the indecomposables of R and satisfy $\mathsf{R}_{i,j} \otimes \mathsf{R}_{j,k} \to \mathsf{R}_{i,k}$. Each **component category** $\mathsf{R}_{i,i}$ is a ring category with unit 1_{R_i} and each $\mathsf{R}_{i,j}$ is a a $\mathsf{R}_{i,i}$-$\mathsf{R}_{j,j}$-bimodule category. This leads to an interpretation as the 2-category with a 0-cell for each i, a 1-cell from i to j for each object of $\mathsf{R}_{i,j}$ and a 2-cell for each morphism of R. Physically the 0-cells can represent topological phases, 1-cells domain walls between phases and 2-cells junctions of domain walls.

The Grothendieck ring $K_0(\mathsf{R})$ of a multiring category is an **$\mathbb{N}$-ring** (i.e. a free $\mathbb{Z}$-module on the equivalence classes of indecomposables with nonnegative structure constants) with unit element $[1_{\mathsf{R}}] = \sum_i [1_{\mathsf{R}_i}]$. The structure constants N_{ab}^c determine the **fusion rules**

$$a \times b = \sum_c N_{ab}^c c$$

for each pair a, b of equivalence classes of indecomposables.

The book [11] calls a faithful and exact linear functor $F : \mathsf{R} \to \mathsf{S}$ between multiring categories a **quasi-tensor functor** if

$$F(-) \otimes F(-) \simeq F(- \otimes -)$$

and $F(1_{\mathsf{R}}) = 1_{\mathsf{S}}$. Each quasi-tensor functor $F : \mathsf{R} \to \mathsf{S}$ between multi-ring categories induces a ring homomorphism $K_0(\mathsf{R}) \to K_0(\mathsf{S})$. A monoidal functor between multiring categories is a **tensor functor**. Every tensor functor is quasi-tensor.

If R has left duals then 1_{R} is semisimple with simple components 1_{R_i}.

0.4.2 Multitensor categories

A **multitensor category** is a rigid multiring category, or equivalently, an Artinian linear abelian rigid monoidal category with bilinear tensor product [11]. Rigidity implies biexactness of $\otimes$. A **tensor category** is a multitensor category with simple unit, or equivalently, a rigid ring category.

Left and right duals are isomorphic in a semisimple multitensor category over an algebraically closed field ([11] Proposition 4.8.1). So each object a has a well-defined squared dimension $|a|^2$, which can be computed relative to any isomorphism $a \to a^{**}$ but is independent of the choice. It is however an open question whether such a choice can always be made naturally, i.e. whether such categories always have a pivotal structure i.e. commute with $\otimes$.

The Grothendieck ring $K_0(\mathsf{T})$ of a multitensor category is a **based ring**, i.e. an $\mathbb{N}$-ring with involution.

Recall that Definition 8.10.1 of [11] defined a twist on a rigid braided category B to be a natural isomorphism $\theta \in \mathrm{End}(\mathrm{id}_{\mathsf{B}})$ satisfing (1). Definition 8.10.1 of [11] further calls θ a **ribbon structure** if $\theta_{a^*} = \theta_a^*$ for all a and calls B a **ribbon tensor category** if so equipped.

Exercise 0.4.1 Verify that this yields a multitensor category by using the ribbon structure to recover biexactness of the tensor product.

0.4.3 Multifusion categories

A **multifusion category** is a semisimple multitensor category with finitely many isomorphism classes of simple objects. A **fusion category** is a semisimple tensor category with finitely many isomorphism classes of simple objects, i.e. a multifusion category with a simple unit.

The Grothendieck ring $K_0(\mathsf{F})$ of a fusion category F is a finite-rank based ring and is also known as a **fusion ring**. There can be only finitely many fusion categories with a given fusion ring by Ocneanu rigidity.

Let $\mathrm{FPdim}(a)$ be the top eigenvalue of the **fusion matrix** $N_a \in \mathbb{N}^{n\times n}$, which encodes the fusion rules via $(N_a)_{cb} = N_{ab}^c$. By the Frobenius-Perron Theorem, the corresponding eigenspace is spanned by the all 1s vector. The **Frobenius-Perron dimension** is

$$\mathrm{FPdim}(\mathsf{F}) = \sqrt{\sum_a \mathrm{FPdim}(a)^2}.$$

The **categorical dimension** is defined as

$$\dim(\mathsf{F}) = \sqrt{\sum_a |a|^2}.$$

Then $\mathcal{D} \leq \mathrm{FPdim}(\mathsf{F})$ and if equality holds F is called **pseudo-unitary**.

In a braided fusion category with a twist θ, the pivotal structure $\theta \circ u$ is spherical iff the θ is a ribbon structure (Proposition 8.10.12).

Each pseudo-unitary fusion category has a canonical spherical structure with $\mathrm{Pdim}(a) = \mathrm{FPdim}(a)$ for all objects a ([11] Proposition 9.5.1).

Unitary implies pseudounitary [11].

Bannai observed [13] that fusion rings are essentially the same thing as the association schemes studied in combinatorics. See Section X.4.

0.4.4 Premodular categories

In a braided fusion category F with a twist, the left/right pivotal traces of the full twist $R_{ba}R_{ab}$ define the S-**matrix**

$$S_{ab} = (\mathrm{PTr}_L \otimes \mathrm{PTr}_R)(R_{ba}R_{ab}).$$

The pivotal structure is spherical iff the twist is ribbon, so spherical braided fusion categories and ribbon fusion categories are the same thing, also known as a **premodular category**. In a premodular category, the fusion matrices N_a are normal and mutually commuting. The S-matrix is symmetric with S_{i0} and S_{0i} equal to the Pdims, which equal the FPdims under the pseudo-unitary spherical structure described above.

The **Gauss sums** ([11] 8.15)

$$p^{\pm} = \sum_a \theta_a^{\pm 1} d_a^2$$

of a premodular category satisfy $p^- = \overline{p^+}$ and $p^+p^- = \mathcal{D}^2$, where

$$\mathcal{D} = \sqrt{\sum_a d_a^2} = |p^{\pm}|$$

is the total quantum dimension.

Chapter I
Rings

I.1 Basic definitions

A **ring** is a set A with a commutative addition and an associative product, satisfying the distributive laws and containing 0 and 1 such that $(A, +, 0)$ is an abelian group and $(R \setminus 0, \cdot, 1)$ is a multiplicative monoid. Every ring has $0 \neq 1$ except the **zero ring** $\{0\}$, the unique ring with one element.

If B is a ring and $A \subset B$ is a subset that is also ring, then it is **subring** if $1_A = 1_B$. A **homomorphism** $f : A \to B$ of rings by definition satisfies $f(1_A) = 1_B$, in addition to respecting sums and products. The image $f(A) \subset B$ is always a subring, but the kernel $\ker(f) \subset B$ is only a subring when B is the zero ring. For each $a \in A$, left and right multiplication induce homomorphisms $a\cdot : A \to A$ and $\cdot a : A \to A$ of the underlying additive group of A.

The category Ring of rings has products (the Cartesian product) and coproducts (the free product) but no direct sum. The initial object in Ring is $\mathbb{Z}$ and the final object is the zero ring. A homomorphism is injective iff it is a monomorphism. Surjective homomorphisms are epimorphisms but there are non-surjective epimorphisms such as the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$.

I.2 Elements

Let A be a ring. An element $a \in A$ is a **unit** if it has an inverse a^{-1} for which $aa^{-1} = 1$ (therefore $a^{-1}a = 1$.) The **unit group**

$$A^\times = \{a \in A : ab = ba = 1 \text{ for some } b \in A\}$$

is the multiplicative group of units in A. Each ring homomorphism $f : A \to B$ induces a homomorphism $f : A^\times \to B^\times$ of unit groups. If $A \subset B$ is a subring, then $A^\times \subset B^\times$ is a subgroup. The ring A is a **division ring** if every nonzero element is a unit, i.e. if $A \setminus 0 = A^\times$.

An element $a \in A$ is **left regular** if left multiplication by a is injective. Otherwise, a is a **left zero divisor** as there exists $b \in A$ such that $ab = 0$. We call a **regular** if it is both left regular and right regular, otherwise a **zero divisor** if it is a left zero divisor or a right zero divisor. A ring is a **domain** if every nonzero element is regular, i.e. if 0 is its only zero divisor.

An element a is **nilpotent** if $a^n = 0$ for some $n \geq 1$. So nonzero nilpotents, if they exist, are special kinds of zero divisors. A ring A is **reduced** if it contains no nonzero

nilpotents. The above classes of rings, which are characterized by the corresponding properties of their elements, satisfy the following inclusions:

$$\{\text{division rings}\} \subset \{\text{domains}\} \subset \{\text{reduced rings}\}.$$

The **center** $Z(A)$ of A is the set of elements that commute with every element in A. It is a commutative subring satisfying $Z(A)^\times = Z(A^\times)$. An **algebra** over a commutative ring R, or an R**-algebra**, consists of a ring A together with a homomorphism $R \to Z(A)$. Note that every ring A is canonically a $\mathbb{Z}$-algebra and a $Z(A)$-algebra.

I.3 Modules

A **module** over a ring A is an abelian group M carrying a left action of A, satisfying

$$a(x+y) = ax + ay, \;\; (a+b)x = ax + bx, \;\; (ab)x = a(bx), \;\; 1_A x = x.$$

Equivalently, the left action is given by a homomorphism $A \to \mathrm{End}(M)$. A **right module** over A has a right action satisfying

$$(x+y)a = xa + ya, \;\; x(a+b) = xa + xb, \;\; x(ab) = (xb)a, \;\; x1_A = x,$$

or equivalently, that is given by some antihomomorphism $A \to \mathrm{End}(M)$. Note that for right modules, ab acts first via a, then by b, so we can view a right module as a left module over the **opposite** ring A^{op} in which the order of multiplication is reversed. Given two rings A, B, an A-B**-bimodule** is simultaneously a left A-module and a right B-module with mutually commuting actions. We call an A-A-module an A**-bimodule** and we call a left module a **module**.

Homomorphisms between modules are the additive maps $f : M \to N$ satisfying $f(am) = af(m)$ for all $a \in A$, $m \in M$. They form the morphisms in the category A-mod of A-modules. Similarly, morphisms in the category mod-A of right A-modules satisfy are the homomorphisms $f(ma) = f(m)a$, with a similar definition for bimodules.

The full category A-mod of A-modules is additive (abelian in fact). So we call a module **decomposable**, **indecomposable**, **simple**, **semisimple**, **Noetherian**, **Artinian**, or **finite-length** if it is that kind of object in A-mod.

A module M is indecomposable iff $\mathrm{End}(M)$ is **directly indecomposable** (the only idempotents in $\mathrm{End}(M)$ are 0 and 1) iff $\mathrm{Spec}(\mathrm{End}(M))$ is connected. A module M is called **strongly indecomposable** when $\mathrm{End}(M)$ is a local ring.

Lemma I.3.1 (Schur) A module M is simple iff $\mathrm{End}(M)$ is a division ring. If M and N are simple modules, then $\mathrm{Hom}(M,N) \neq 0$ iff $M \simeq N$.

A module M is simple iff it is cyclic ($M = Am$) iff $M \simeq A/I$ for some maximal right ideal I of A. A proper submodule $N \subset M$ is maximal iff M/N is simple.

simple module ⇒ strongly indecomposable module ⇒ indecomposable module

because

division ring ⇒ directly indecomposable ring ⇒ simple ring.

A module is **semisimple** if it is a direct sum of simple modules.

A module M is **Noetherian** if every sequence

$$\cdots \subset M_{i-1} \subset M_i \subset \cdots$$

of distinct submodules of M has a maximal element (the Ascending Chain Condition (ACC)), **Artinian** if every such sequence has a minimal element (the Descending Chain Condition (DCC)) and of **finite length** if it satisfies both, i.e. is a finite object in A-mod. A module has finite length iff it has a **composition series**, i.e. a finite filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

by distinct submodules satisfying any of the following equivalent conditions:

- Its length n is maximal.
- Each M_i is maximal in M_{i+1}.
- Each M_{i+1}/M_i is irreducible.

Theorem I.3.1 (Jordan-Holder) The isomorphism class of M is uniquely determined by the isomorphism classes of the M_i/M_{i-1}. Furthermore, any other composition series $0 = M'_0 \subset \cdots \subset M'_{n'} = M$ for M must satisfy $n = n'$ and $M'_i/M'_{i-1} \simeq M_{\pi(i)}/M_{\pi(i)-1}$ for some permutation $\pi \in S_n$.

Exercise I.3.1 Show that the following conditions on a module M are equivalent (see [3] for more detail):

- M is semisimple.
- Every submodule of M is a direct summand.
- M is a direct sum of simple modules.
- M is a sum of simple modules.

Exercise I.3.2 Show that the following conditions are equivalent on a semisimple module:

- It is finitely generated.

- It is a finite direct sum of irreducible modules.
- It is Noetherian.
- It is Artinian.
- It is finite.

Exercise I.3.3 Show that a module is Noetherian iff every submodule is finitely generated.

Theorem I.3.2 (Krull-Schmidt) If M is a finite-length module, then M is isomorphic to a direct sum of indecomposable modules that is uniquely determined up to isomorphisms and relabelings.

Using the full abelian category A-mod lets us define further properties of a module. A module is **free** if it is isomorphic to a finite direct sum A^n of copies of A. A module M is **finite** if it is finitely generated, i.e. if there exists an exact sequence

$$A^n \to M \to 0.$$

It is **finitely presented** if the kernel of that homomorphism is finitely generated, i.e. if there is an exact sequence

$$A^m \to A^n \to M \to 0.$$

A module P is **projective** if every exact sequence

$$0 \to M \to N \to P \to 0$$

splits, and a module Q is **injective** if every

$$0 \to Q \to M \to N \to 0$$

splits. A finite-length module M is **stably free** (i.e. $P \oplus A^m \simeq A^n$ for sufficiently large m and n) iff it is projective.

I.3.1 The radical

The **radical** $\mathrm{rad}(M)$ of a module M is the intersection of all maximal submodules of M. If M is finitely generated, then maximal submodules exist by Zorn's lemma, implying that $\mathrm{rad}(M) \neq M$. However, if M is not finitely generated, M need not contain any maximal submodules, in which case the empty intersection $\mathrm{rad}(M) = M$ is possible.

Exercise I.3.4 Prove that every semisimple module has a trivial radical. Note that $\{0\}$ is the only maximal submodule of a simple module.

Exercise I.3.5 Prove that a module is finitely generated and semisimple iff it is Artinian with trivial radical.

More generally, composition series can be defined for objects in any abelian category.

I.3.2 Properties of rings based on modules

A ring is **primitive** if it has a faithful simple module and **semiprimitive** if each nonzero element acts nontrivially on some simple module. Equivalently, it is semiprimitive if it has a faithful semisimple module.

A ring is **left semihereditary** if all submodules of finitely generated modules are projective, and **left hereditary** if this holds for all modules. A ring is **(semi)hereditary** if it is both left and right (semi)hereditary.

I.4 Ideals

Much can be learned about a ring A by viewing it as a module over itself. Submodules of A are **left ideals**, right submodules of A are **right ideals** and bisubmodules of A are **ideals**. Given $a \in A$, write $(a) := AaA$ for the **principal ideal** generated by a.

If $I, J \subset A$ are left ideals, then $I \cap J$ is the largest left ideal contained in I and J, whereas $I + J$ is the smallest left ideal containing I and J. The same holds for right ideals and for ideals. If $I \subset A$ is a left ideal and $J \subset A$ is a right ideal, then IJ is an ideal. Every left ideal of a commutative ring R is an ideal.

The ideals of a ring are analogous to the normal subgroups of a group and satisfy similar isomorphism theorems:

1. Given a homomorphism $f : A \to B$, its kernel $\ker(f) \subset A$ is an ideal and $A/\ker(f) \simeq f(A) \subset B$ is a subring.

2. Given a subring $B \subset A$ and an ideal $I \subset A$, $B+I \subset A$ is a subring and $I \subset B+I$ is an ideal with $(B + I)/I \simeq B/(B \cap I)$.

3. For each ideal $I \subset A$, there is an inclusion-reversing bijection $B \to B/I$ from the subrings $I \subset B \subset A$ to the subrings of A/I, inducing a bijection $J \mapsto J/I$ from the intermediate ideals $I \subset J \subset A$ to the ideals of A/I. In particular, B is an ideal of A iff $B/I \subset A/I$ is an ideal.

I.4.1 Types of ideals

A proper (left) ideal $M \subset A$ is a **maximal (left) ideal** if it is not contained in any larger proper (left) ideal. A ring A is **simple** if it containes *exactly* two ideals: the zero ideal (0) and A itself. Equivalently, A is simple iff (0) is a maximal ideal. Furthermore, if A is any ring, an ideal $M \subset A$ is maximal iff A/M is a simple ring.

An ideal $P \subset A$ is **prime** if $IJ \subset P \Rightarrow I \subset P$ or $J \subset P$ holds for all ideals $I, J \subset A$. It is however sufficient to check the condition only left ideals or right ideals, or even on principal ideals, where it simplifies to $aAb \subset P \Rightarrow a \in P$ or $b \in P$. A ring A is **prime** if $aAb = 0$ implies $a = 0$ or $b = 0$; equivalently, A is a prime ring iff (0) is a prime ideal. Furthermore, $P \subset A$ is a prime ideal iff A/P is a division ring.

Call a subset $S \subset A$ an **m-system** if, for every $a, b \in S$, there exists a $c \in A$ such that $acb \in S$, i.e. if $S \cap aAb \neq \emptyset$. If A is commutative, then an m-system is just a multiplicative set. An ideal $P \subset A$ is prime iff $A \setminus P$ is an m-system iff P is maximal among all proper ideals disjoint from some m-system S. This implies that every maximal ideal is prime, though non-maximal prime ideals can exist in general.

An ideal $C \subset A$ is **completely prime** if $ab \in C \Rightarrow a \in C$ or $b \in C$. An ideal C is completely prime iff A/C is a domain.

An ideal $Q \subset A$ is **semiprime** if $I^2 \subset Q$ implies that $I \subset Q$. As with prime ideals, it again suffices to check this on one-sided or even principal ideals, where it simplifies to $aAa \subset Q \Rightarrow a \in Q$. It can be shown that Q is semiprime iff it is an intersection of prime ideals. Call a subset $N \subset A$ **nilpotent** if $N^n = \{0\}$ for some $n \geq 1$, and a ring **semiprime** if it contains no nonzero nilpotent one-sided ideals. Then A is semiprime iff (0) is a semiprime ideal.

Exercise I.4.1 Show Q is semiprime iff A/Q is reduced.

Question I.4.1 Does reduced also mean trivial nil*?? Note that trivial nil$_*$ means semiprime so this is consistent with reduced $\Rightarrow$ semiprime.

Call a subset $S \subset A$ an **n-system** if $aAa \cap S \neq \emptyset$ for every $a \in A$. Then Q is semiprime iff $A \setminus Q$ is an n-system.

The three classes of rings defined above generalize those defined earlier at the level of ideals rather than individual elements:

$$\begin{array}{ccccc} \{\text{simple rings}\} & \subset & \{\text{prime rings}\} & \subset & \{\text{semiprime rings}\} \\ \cup & & \cup & & \cup \\ \{\text{division rings}\} & \subset & \{\text{domains}\} & \subset & \{\text{reduced rings}\} \end{array}$$

In the next section these are further generalized by considering the modules over A, to primitive and semiprimitive rings, the latter of which encompasses most, if not all of the rings we consider.

I.4.2 Primitive ideals

The **annihilator**

$$\mathrm{Ann}(M) = \{a \in A : aM = 0\}$$

of an A-module M is an ideal because it is the kernel of the homomorphism $A \to \mathrm{End}_{\mathbb{Z}}(M)$ defined by the action of A of M. An ideal is **primitive** if it is the annihilator of a simple module.

Exercise I.4.2 Show that primitive ideals are prime.

A ring A is called **primitive** if it has a faithful simple module.

Exercise I.4.3 ([3] (11.4)) Show that an ideal is primitive iff A/I is primitive.

Similar definitions can be made regarding the right action.

I.4.3 Radicals and nilpotency

Given an ideal $I \subset A$, define its **prime radical** to be the intersection

$$\sqrt{I} = \bigcap\{\text{prime ideals } P \supset I\}$$

of the prime ideals containing I. An ideal $Q \subset A$ is therefore semiprime iff $\sqrt{Q} = Q$ iff Q is an intersection of prime ideals. The **lower nilradical**[1]

$$\mathrm{nil}_*(A) = \bigcap\{\text{prime ideals } P \subset A\} = \sqrt{(0)},$$

is therefore the smallest semiprime ideal.

A subset $N \subset A$ is called **nil** if all its elements are nilpotent. Sums of nil ideals are nil, so there is a largest nil ideal: the **upper nilradical**

$$\mathrm{nil}^*(A) = \sum\{\text{nil ideals } N \subset A\}.$$

Köthe conjectured in 1930 that the sum of two nil left ideals is nil, or equivalently, that if (0) is the only nil ideal, it is the only nil left ideal. Another formulation of the conjecture is that $\mathrm{nil}^*(A) = 0$ should imply there are no nonzero nil left ideals. Surprisingly, the conjecture is still open. The conjecture is true for rings admitting an involution inducing a nondegenerate norm (i.e. $a^*a = 0 \Rightarrow a = 0$).

A sufficient condition for a (left) ideal $N \subset A$ to be nil is that is be **nilpotent**, meaning that $N^n = (0)$ for some n. Note that nilpotent $\Rightarrow$ nil by definition. Sums of nilpotent ideals can fail to be nilpotent in noncommutative non-Noetherian rings.

[1] a.k.a. Baer's radical, Baer-McCoy radical, prime radical

For any ring A,

$$\mathrm{nil}_*(A) \subset \mathrm{nil}^*(A) \subset \mathrm{rad}(A),$$

where $\mathrm{rad}(A)$ is the **Jacobson radical**

$$\begin{aligned} \mathrm{rad}(A) &= \bigcap\{\text{maximal left ideals of } A\} \\ &= \{a \in A : 1 + Aa \subset A^\times\} \\ &= \{a \in A : 1 + AaA \subset A^\times\} \\ &= \{a \in A : 1 + aA \subset A^\times\} \\ &= \bigcap\{\text{maximal right ideals of } A\}. \end{aligned}$$

Exercise I.4.4 Show that the Jacobson radical $\mathrm{rad}(A)$ can also be written as the intersection of left primitive or right primitive ideals.

A ring A is **semiprimitive** if it has a faithful semisimple module.

Exercise I.4.5 Show that a ring A is semiprimitive iff $\mathrm{rad}(A) = 0$.

Such rings are therefore also known as **semisimple in the sense of Jacobson**, **J-semisimple**, and in some earlier literature ([1] e.g.) just semisimple.

I.5 Finiteness conditions on rings

A ring is **left/right-Noetherian/Artinian** if it is Noetherian/Artinian as a left/right module over itself. A ring is **Noetherian/Artinian** if it is both left and right Noetherian/Artinian. A ring is **simple/semisimple** according to whether it is in its own category of bimodules.

I.5.1 Noetherian rings

A ring is **left Noetherian** if it a Noetherian module over itself, **right Noetherian** if it is a Noetherian right module over itself, and **Noetherian** if it is both left and right Noetherian.

Exercise. Show that the following conditions on a ring are equivalent:

- It is left Noetherian
- Every left ideal is finitely generated
- Direct sums of injectives are injective
- Every injective is a sum of injective indecomposables

Example. Show that $\left(\begin{smallmatrix}\mathbb{Z} & \mathbb{Q}\\ 0 & \mathbb{Q}\end{smallmatrix}\right)$ is right Noetherian but not left Noetherian.

While nilpotent ideals are always nil, **Levitzky's Theorem** says that if A is a left Noetherian ring, then every nil ideal of A is nilpotent and there exists a largest nilpotent ideal, the **nilradical**

$$\mathrm{nil}(A) = \mathrm{nil}_*(A) = \mathrm{nil}^*(A).$$

Theorem I.5.1 (Hilbert's Basis Theorem) If A is left Noetherian, then so is the polynomial ring $A[x]$.

Exercise I.5.1 Show that if A is Noetherian and $I \subset A$ is an ideal, then A/I is Noetherian. Use Hilbert's Basis Theorem to conclude that finitely generated algebras over commutative Noetherian rings are Noetherian.

Non-Noetherian rings include polynomial rings $\mathbb{Z}[x_1, x_2, \dots]$ in infinitely many variables and the ring $\mathbb{A} = \prod_v' \mathbb{Q}_v$ of ideles.

I.5.2 Artinian rings

A ring is **left Artinian** if it an Artinian module over itself, **right Artinian** if it is an Artinian right module over itself, and **Artinian** if it is both left and right Artinian.

Exercise I.5.2 Show that the following conditions on a ring are equivalent:

- It is left Artinian.
- Every left ideal contains a minimal left ideal.
- Direct sums of projectives are projective.
- Every projective is a sum of projective indecomposables.

Some years after Artin defined Artinian rings, Akizuki-Hopkins-Levitzky proved that left-Artinian rings are left Noetherian. If A is a left-Artinian ring, then all its radicals coincide:

$$\mathrm{nil}(A) = \mathrm{nil}_*(A) = \mathrm{nil}^*(A) = \mathrm{rad}(A).$$

Exercise I.5.3 Use the Jacobson radical to prove the Akizuki-Hopkins-Levitzky Theorem.

Exercise I.5.4 Show that a simple ring is left Artinian iff it is right Artinian iff it is isomorphic to $D^{n\times n}$ for some division ring D.

Exercise I.5.5 Show that $\mathbb{Z}$ is Noetherian but not Artinian, whereas $\mathbb{Q}$ is both Artinian and Noetherian.

I.5.3 Semisimple rings

A ring is **semisimple** if it is semisimple as a left module over itself.

Exercise I.5.6 Show that the following conditions on a ring are equivalent:

- It is semisimple.
- Every module is semisimple.
- Every finitely generated module is semisimple.
- Every cyclic module is semisimple.
- Every short exact sequence of modules splits.
- Every module is projective.
- Every finitely generated module is projective.
- Every cyclic module is projective.

Example I.5.1 The matrix ring $\mathbb{C}^{2\times 2}$ is simple but not semisimple, because it contains the nontrivial left ideal $\left(\begin{smallmatrix} 0 & \mathbb{C} \\ 0 & \mathbb{C} \end{smallmatrix}\right)$.

The following important structure theorem shows that a ring is semisimple iff its opposite is, so there is no need to separately consider *left semisimple* rings.

Theorem I.5.2 (Artin-Wedderburn) A ring is semisimple iff it is isomorphic to a finite direct product $\prod_i D_i^{n_i \times n_i}$ of matrices over division rings D_i.

Proof. See [3] 3.5. The "if" direction is trivial. As a module over itself, a semisimple ring by definition decomposes as a direct sum of minimal left ideals, finitely many because A is Noetherian. These minimal left ideals can be shown to be two sided, proving the "only if" direction. □

Wedderburn first proved this for finite-dimensional semisimple algebras over fields in his 1907 Ph.D. thesis. A key step in his proof showed that a finite-dimensional algebra A is semisimple iff it has no nontrivial nilpotent ideal iff $\mathrm{rad}(A) = 0$. The proof generalizes to Artinian rings, for which $\mathrm{rad}(A) = 0$ implies semisimplicity. Confusingly, some sources ([1], [14], Wikipedia) call a ring semisimple if its Jacobson radical is trivial,

and thus call our semisimple rings "Artinian semisimple rings." It is now standard to call rings with trivial radical *semisimple in the sense of Jacobson*, **J-semisimple** or **semiprimitive**, in which case semisimple = Artinian J-semisimple.

A commutative simple ring is a field, and a commutative semisimple ring is a finite direct product of fields.

I.6 Examples

I.6.1 Weyl algebras

If A is an algebra, the **Weyl algebra** $A_1(A) = A[X, P]/(PX - XP - 1)$ where X and P are noncommuting "position" and "momentum" variables. The n**th Weyl algebra** is defined recursively $A_n(A) = A_1(A_{n-1}(A))$. The Weyl algebra $A_n(A)$ is not Artinian because the monomials X^n generate a strictly decreasing infinite sequence of ideals. On the other hand it is Noetherian/simple/a domain iff A is.

The Weyl algebra $A_1(R) = R[x_1, \ldots, x_n, \partial_1, \ldots, \partial_n]$ over a commutative ring A is isomorphic to the algebra of derivations of the polynomial algebra $R[x_1, \ldots, x_n]$. The Weyl algebra $A_n(k)$ over a field k of characteristic 0 is a hereditary non-Artinian simple Noetherian domain [CITATION?].

The Weyl algebra is related to the universal enveloping algebra of the Heisenberg Lie algebra and the affine Lie algebra $\widehat{\mathfrak{u}}_1$.

The universal enveloping algebra $U(\mathfrak{g})$ of a nontrivial Lie algebra $\mathfrak{g}$ is non-Artinian, Noetherian and J-semisimple.

`https://math.stackexchange.com/questions/3615836/semisimple-lie-algebra-and-jacobson-radical`

I.7 Types of rings

ring	simple	semisimple	J-semisimple	left/right Artinian	left/right Noetherian
$\mathbb{Q}$	yes	yes	yes	yes	yes
$\left(\frac{-1,-1}{\mathbb{R}}\right)$	yes	yes	yes	yes	yes
$\mathbb{Z}$	no	no	yes	no	yes
$\mathbb{Z}[\boldsymbol{i},\boldsymbol{j}]$	no	no	?	no	yes
A_n(simple ring)	yes	no	yes	no	yes
$U(\mathfrak{g}_{\text{simple}})$	yes	no	yes	no	yes

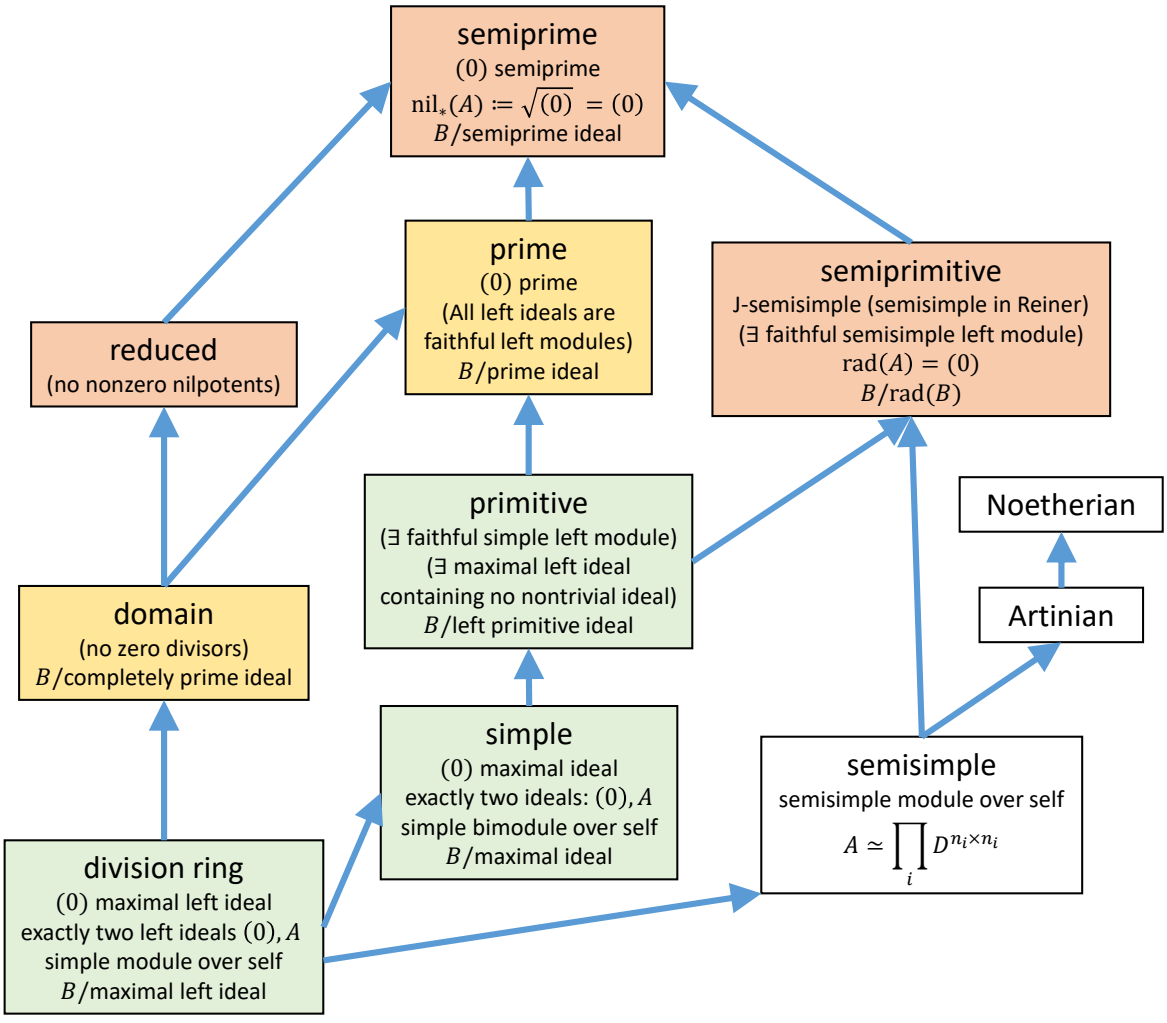


Figure I.1: Types of rings. A = that kind of ring, B = any ring. Colored types coincide for commutative rings.

I.8 Graded rings

A ring A is **graded** by a group G, or G-graded, if its additive group splits as a direct sum

$$A = \bigoplus_{g \in G} A_g$$

such that $A_g A_{g'} \subset A_{gg'}$.

If A is G-graded and B is H-graded, then $A \times B$ is $G \times H$-graded. If $H = G$, define a G-grading on $A \times B$ such that

$$(A \times B)_g = \bigoplus_{xy=g} A_x \times B_y.$$

Examples: polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ is $\mathbb{Z}$-graded and $\mathbb{Z}^n$-graded. Group ring $\mathbb{C}G$ is G-graded by definition.

$\mathbb{Z}/2$-graded rings and algebras are also known as **superalgebras**.

Homogeneous ideals and (multi)Proj, noncommutative Proj, noncommutative algebraic geometry, example: noncommutative line.

I.9 Local rings

A ring A is a **local ring** if it satisfies any of the following equivalent conditions ([3] 19.1):

1. A has a unique maximal left ideal
2. A has a unique maximal right ideal
3. the non-units $A \setminus A^\times$ form an ideal
4. the non-units $A \setminus A^\times$ form an abelian group
5. for every $a \in A$, either $a \in A^\times$ or $1 - a \in A^\times$
6. $a_1 + \cdots + a_n \in A^\times \Rightarrow a_i \in A^\times$ for some i.
7. $a + b \in A^\times \Rightarrow a \in A^\times$ or $b \in A^\times$
8. A decomposes as a disjoint union $A = A^\times \cup \operatorname{rad}(A)$
9. $A/\operatorname{rad}(A)$ is a division ring

The maximal left ideal and maximal right ideal of a local ring A coincide and are equal to the Jacobson radical $\operatorname{rad}(A)$, which is also the unique maximal ideal of A. Although a ring with a unique maximal ideal is not necessarily local, the center of such a ring is a local ring [1]. [3] defines A to be **semilocal** ([3] §20) if $A/\operatorname{rad}(A)$ is left Artinian (equivalently, semisimple). Simple/semisimple versus division ring/prime ring?

Other definitions: completeness, DVR, valuations, places, etc. Localizations versus completions.

A finite-length module M is indecomposable iff $\operatorname{End}(M)$ is a local ring. If a general module M is indecomposable, then $\operatorname{End}(M)$ is a local ring.

A commutative ring R is a DVR if it is a PID with a unique prime (or equivaelntly, maximal) ideal $\mathfrak{p} = A\pi$.

I.9.1 Valuations and completions

An **absolute value** on a field K is a function $|\cdot|\colon K \to \mathbb{R}$ such that $|x| = 0$ iff $x = 0$ and

$$|xy| = |x| \cdot |y|, \;\; |x+y| \leq \max\{|x|, |y|\} \text{ with equality iff } x \neq y.$$

An absolute value is **archimedean** if it further satisfies $|x+y| \leq |x|+|y|$ and otherwise it is **nonarchimedean**. Ostrowski's theorem states that if K is complete with respect to an archimedean absolute value, then K is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$.

More generally, a **valuation** on a field K is a function v such that $v(K^\times)$ is a totally ordered abelian group (the **value group**) with $v(0)$ extremal. If the value group is multiplicative, this is essentially the same as an absolute value. If the value group is additive (such as for a **discrete valuation**, where $v(K^\times) \simeq \mathbb{Z}$), then $v(x) = \infty$ iff $x = 0$ and

$$v(xy) = v(x) + v(y), \;\; v(x+y) \geq \min\{v(x), v(y)\} \text{ with equality iff } x \neq y.$$

The conditions that an absolute value be **normalized** are as follows: If v is real, then $|x|_v = |\iota_v(x)|$, where $\iota_v\colon K \to \mathbb{R}$ is the corresponding real embedding. If v is complex, then $|x|_v = |\iota_v(x)|^2 = \iota_v(x)\bar{\iota}_v(x)$, where $\iota_v, \bar{\iota}_v\colon K \to \mathbb{C}$ are the two embeddings associated to v, related by complex conjugation. If v is a nonarchimedean absolute value on a number field corresponding to the finite prime $\mathfrak{p}$, then $|x|_v = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-\operatorname{ord}_\mathfrak{p}(x)}$. Every $x \in K^\times$ satisfies the **product formula** $\prod_v |x|_v = 1$, where the product is over all places and the absolute values are normalized.

I.10 Associative algebras

Let R be a commutative ring. In these notes (and elsewhere), a **algebra** is a ring A equipped with a homomorphism $R \to Z(A)$ from a commutative ring R into its center. We may then write A/R or call A an **R-algebra** or an **algebra over** R when the **base ring** R needs to be specified. Note that "ring" is synonomous with "$\mathbb{Z}$-algebra." Furthermore, every ring A is a $Z(A)$-algebra. In particular, "algebra" without further qualifiers = "unital associative algebra."

Left ideals, **right ideals** and **ideals** of an R-algebra A are defined relative to the underlying ring. In each case, they are R-submodules of A because R maps into the center of A. Call an algebra **simple** if its underlying ring is simple and **semisimple** if its underlying ring is semisimple. An R-algebra is **central** if its center is isomorphic to R. In particular, every ring A is a central $Z(A)$-algebra.

An R-algebra A is **separable** if it is a projective module over its **enveloping algebra** $A \otimes_R A^{\mathrm{op}}$. The enveloping algebra acts on A via $(\sum a_i \otimes a_i') \cdot x = \sum a_i x a_i'$ and its product satisfies $(\sum a_i \otimes a_i')(\sum b_j \otimes b_j') = \sum (a_i b_j) \otimes (b_j' a_i')$. A central separable algebra is called an **Azumaya algebra**.

If A/K is a commutative algebra over a field, then A is a field if it is simple, a finite direct product of fields if it is semisimple, and an étale algebra if it is separable.

Chapter II
Schemes

II.1 Commutative rings

Let R be a commutative ring. Then all ideals are two sided and many of the classes of noncommutative rings collected in Figure I.7 coincide:

- **field** = division ring = simple = primitive
- **integral domain** = prime
- **reduced** = semiprime = semiprimitive = J-semisimple.

The corresponding statements about ideals are

- A proper subset $\mathfrak{m} \subset R$ is a maximal ideal iff it is a maximal left ideal.
- A proper ideal $\mathfrak{p} \subset R$ is prime iff it is completely prime iff $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.
- There is a largest nilpotent ideal, or **nilradical**

$$\mathrm{nil}(R) = \mathrm{nil}_*(R) = \mathrm{nil}^*(R) = \mathrm{rad}(R).$$

II.2 Sheaves

A **presheaf** on a category C is a contravariant functor $\mathcal{F} : \mathsf{C} \to \mathsf{Set}$. A precosheaf is a covariant functor $\mathcal{F} : \mathsf{C} \to \mathsf{Set}$.

II.2.1 Topological spaces

The open sets $\mathsf{Open}(X)$ of a topological space X are closed under union and finite intersection, where by convention the empty intersection is X. A subset $B' \subset \mathsf{Open}(X)$ is a **subbase** if it generates the topology, i.e. is the smallest topology containing B'. Equivalently B' is a subbase if every open set is a union of finite intersections of sets in B'. A subset $B \subset \mathsf{Open}(X)$ is a **base** if every open set is a union of sets in B. Equivalently, B is a base if finite intersections of sets in B are unions of sets in B. In particular, B' is a subbase iff its closure under all finite intersections is a base.

Exercise II.2.1 A map $f : X \to Y$ between topological spaces is an **open mapping** if it restricts to a functor $\mathsf{Open}(X) \to \mathsf{Open}(Y)$ and **continuous** if $f^{-1} : \mathsf{Open}(Y) \to \mathsf{Open}(X)$ is a contravariant functor.

A subset U of a topological space X is **reducible** if $U = U_1 \cup U_2$ for closed proper subsets $U_i \subset U$ and is otherwise **irreducible**. The **irreducible components** of a space are its maximal irreducible subsets.

A **neighborhood** of a point is a set containing an open set containing that point. Two points are **topologically distinguishable** if they have a pair of distinct neighborhoods and furthermore **separated** if each has a neighborhood not containing the other.

A space is

- T_0, or **Kolmogorov**, if every two distinct points are topologically distinguishable.
- R_0, or a **symmetric space**, if every two topologically distinguishable points are separated.
- T_1 if every two points are separated. Such spaces are also called **separated**, **accessible** or **Fréchet**. Definition chasing shows a space is T_1 iff it is T_0 and R_0 iff all singletons (equivalently, finite subsets) are closed.
- T_2, or **Hausdorff**, if every two points have a pair of disjoint neighborhoods.

A topological space is T_2, or **Hausdorff**, if any two points have disjoint neighborhoods. Smooth manifolds and in particular Euclidean spaces are T_2 so this condition is familiar. The irreducible components (and therefore the irreducible sets) of a T_2 space are singletons.

Exercise II.2.2 Let $X = \{x, y\}$. There are three possibilities up to isomorphism:

- Suppose the only open sets are X and ϕ. Show that X is R_0 but not T_0.
- Suppose that $\{x\}$ is open but $\{y\}$ is not. Show that X is T_0 but not R_0.
- Suppose both $\{x\}$ and $\{y\}$ are open. Show that X is T_2 (therefore T_1)

II.2.2 Presheaves on a topological space

A **presheaf** on a topological space X is a contravariant functor from the underlying category (poset in fact) of open sets to Set. In other words, it is a map $U \mapsto \mathcal{F}(U)$ from open sets to sets together with restriction maps $\mathrm{res}_{U,V} : \mathcal{F}(U) \to \mathcal{F}(V)$ to each open $V \subset U$ such that $\mathrm{res}_{U,U}$ is the identity and such that for every $W \subset V \subset U$, the

following diagram commutes:

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\quad\mathrm{res}_{U,W}\quad} & \mathcal{F}(W) \\ & {\scriptstyle \mathrm{res}_{U,V}} \searrow \quad \nearrow {\scriptstyle \mathrm{res}_{V,W}} & \\ & \mathcal{F}(V). & \end{array}$$

The **stalk** of $\mathcal{F}$ at x is the set $\mathcal{F}_x$ of equivalence classes of pairs (U, s) with U open and $s \in \mathcal{F}(U)$ for the equivalence relation $(U, s) \sim (V, t)$ iff $s|W = t|W$ for some open $W \subset U \cap V$. Equivalently, the stalk at x is the direct limit = filtered colimit

$$\mathcal{F}_x = \varinjlim_{U \ni \mathfrak{p}} \mathcal{F}(U).$$

The morphisms $\phi : \mathcal{F} \to \mathcal{G}$ in the category $\mathsf{PShv}(X)$ of presheaves on X are the natural transformations between the corresponding contravariant functors to Set. Such a morphism is explicitly given by a collection $\phi(U) : \mathcal{F}(U) \to \mathcal{G}(U)$ of maps that is compatible with restriction in the sense that

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\phi(U)} & \mathcal{G}(U) \\ \downarrow{\scriptstyle \mathrm{res}_{U,V}} & & \downarrow{\scriptstyle \mathrm{res}_{U,V}} \\ \mathcal{F}(V) & \xrightarrow{\phi(V)} & \mathcal{F}(V) \end{array}$$

for open $U \supset V$.

II.2.3 Continuous maps of presheaves

`https://stacks.math.columbia.edu/tag/008C`

A continuous map $f : X \to Y$ determines a **pushforward functor**

$$f_* : \mathsf{PShv}(X) \to \mathsf{PShv}(Y)$$

via $(f_*\mathcal{F})(V) = \mathcal{F}(f^{-1}(U))$. Pushforwards take stalks to stalks, i.e. there is a natural morphism $(f_*\mathcal{F})_{f(x)} \to \mathcal{F}_x$. The map f_* is a morphism from presheaves on X to presheaves on Y.

The **pullback functor**

$$f^* : \mathsf{PShv}(Y) \to \mathsf{PShv}(X)$$

(Stacks writes this f_p) is the left adjoint of the pushforward and is the unique functor such that $(f^*\mathcal{G})(U)$ is the inverse limit of $\mathcal{G}(V)$ over all open U, V with $f(U) \subset V$.

II.2.4 Sheaves on topological spaces

A **sheaf** is a presheaf $\mathcal{F}$ for which every open cover $\{U_i\}$ of X satisfies the following conditions:

- (Equality) If $s, t \in \mathcal{F}(X)$ satisfy $s|_{U_i} = t|_{U_i}$ for all i, then $s = t$.
- (Gluing) If there exist local sections $s_i \in \mathcal{F}(U_i)$ that agree on the overlaps $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$ for all i, j, then there exists a global section $s \in \mathcal{F}(X)$ with $s|_{U_i} = s_i$.

Morphisms of sheaves are morphisms of their underlying presheaves, so there is an inclusion functor

$$\iota : \mathsf{Shv}(X) \to \mathsf{PShv}(X).$$

The left adjoint to ι exists and is called **sheafification**

$$\sharp : \mathsf{PShv}(X) \to \mathsf{Shv}(X)$$

with $\mathcal{F}^\sharp(U)$ containing the $(s_u) \in \bigcup_{u \in U} \mathcal{F}_u$ such that each u has an open neighborhood $u \subset V \subset U$ on which there exists a section $s \in \mathcal{F}(V)$ such that $s_u \sim (V, s)$.

$$\mathrm{Hom}_{\mathsf{PShv}(X)}(\mathcal{F}, \iota(\mathcal{G})) \simeq \mathrm{Hom}_{\mathsf{Shv}(X)}(\mathcal{F}^\sharp, \mathcal{G})$$

Let $f : X \to Y$ be a continuous map. If $\mathcal{F}$ is a sheaf on X, then its pushforward $f_*\mathcal{F}$ is a sheaf on Y, so the pushforward of presheaves restricts to a functor

$$f_* : \mathsf{Shv}(X) \to \mathsf{Shv}(Y)$$

on sheaves. However, if $\mathcal{G}$ is a sheaf on Y, its pullback $f^*\mathcal{G}$ may fail to be a sheaf on X. The **inverse image sheaf** $f^{-1}\mathcal{G} = (f^*\mathcal{G})^\sharp \in \mathsf{Shv}(\mathsf{X})$ is the sheafification of the pullback presheaf and is sometimes called the "pullback sheaf" (e.g. in Stacks) but this can mean other things too. Therefore

$$\cdot^{-1} : \mathsf{Shv}(Y) \to \mathsf{Shv}(X)$$

as required. The adjoint pairs (ι, f^{-1}) and (f_*, f^*) give functorial (in $\mathcal{F}$ and $\mathcal{G}$) bijections

$$\mathrm{Hom}_{\mathsf{Shv}(X)}(f^{-1}\mathcal{G}, \mathcal{F}) \simeq \mathrm{Hom}_{\mathsf{PShv}(X)}(f^*\mathcal{G}, \mathcal{F}) \simeq \mathrm{Hom}_{\mathsf{PShv}(Y)}(\mathcal{G}, f_*\mathcal{F}) \simeq \mathrm{Hom}_{\mathsf{Shv}(Y)}(\mathcal{G}, f_*\mathcal{F}).$$

There are also bijections with the set of f**-maps** $\xi : \mathcal{G} \to \mathcal{F}$ [Stacks Definition 6.21.7] and also with the set of $\mathrm{Hom}_{YX}(\mathcal{G}, \mathcal{F})$ of compatible collections $\phi_{VU} : \mathcal{G}(V) \to \mathcal{F}(U)$ of morphisms over open sets $U \subset X, \pi(U) \subset V \subset Y$ such that

$$\begin{array}{ccc} \mathcal{G}(V) & \xrightarrow{\phi_{VU}} & \mathcal{F}(U) \\ \downarrow{\scriptstyle \mathrm{res}_{V,V'}} & & \downarrow{\scriptstyle \mathrm{res}_{U,U'}} \\ \mathcal{G}(V') & \xrightarrow{\phi_{V'U'}} & \mathcal{F}(U') \end{array}$$

commutes whenever $U' \subset U$ and $f(U') \subset V' \subset V$. See [[15] 2.7B], [Stacks Lemma 6.21.8].

II.2.5 Ringed spaces

A **ringed space** $(X, \mathcal{O}_X)$ is a topological space X equipped with a sheaf of commutative rings, the **structure sheaf** $\mathcal{O}_X$. $\mathcal{O}_X$-modules $\mathcal{M}$ are themselves sheaves on X, i.e. $\mathcal{M}(U)$ is an $\mathcal{O}_X(U)$-module for open $U \subset X$.

A morphism of ringed spaces consists of a continuous map $f : X \to Y$ of the underlying topological spaces together with an f-map $\xi : \mathcal{O}_Y \to \mathcal{O}_X$, or equivalently, a map $f^{-1}\mathcal{O}_Y \to \mathcal{O}_X$ in $\mathsf{Shv}(Y)$ or a map $f^\sharp : \mathcal{O}_Y \to f_*\mathcal{O}_X$ in $\mathsf{Shv}(X)$ (as on p. 72 of [16]). See Section II.2.4 of these notes, or .

II.2.6 Locally ringed spaces

A **locally ringed space** is a ringed space $(X, \mathcal{O}_X)$ whose stalks $\mathcal{O}_{X,x}$ are local rings. We write $\mathfrak{m}_x \subset \mathcal{O}_{X,x}$ for the maximal ideal and $\kappa(x) = \mathcal{O}_{X,x}/\mathfrak{m}_x$ for the **residue field** at x. For example, a smooth manifold equipped with its sheaf of smooth functions is a locally ringed space. Our main examples will be Spec(R) below.

A **morphism** $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ of locally ringed spaces is a morphism of ringed spaces inducing a morphism $f^\sharp : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ of local rings on each stalk, by definition taking the maximal ideal $\mathfrak{m}_{f(x)}$ of $\mathcal{O}_{Y,f(x)}$ to the maximal ideal $\mathfrak{m}_x$ of $\mathcal{O}_{X,x}$.

II.3 Spec(R)

The **prime spectrum** of R is the set Spec(R) of prime ideals of R equipped with the **Zariski topology**. The closed sets

$$V(I) = \{\mathfrak{p} \in \mathrm{Spec}(R) : I \subset \mathfrak{p}\}$$

are determined by the ideals $I \subset R$ and satisfy

$$V(I+J) = V(I) \cap V(J), \;\; V(I \cap J) = V(IJ) = V(I) \cup V(J).$$

The corresponding open sets

$$D(I) = \{\mathfrak{p} \in \mathrm{Spec}(A) : I \not\subset \mathfrak{p}\}$$

satisfy

$$D(I+J) = D(I) \cup D(J), \;\; D(I \cap J) = D(IJ) = D(I) \cap D(J).$$

Furthermore, $I|J$ iff $J \subset I$, in which case $V(I) \subset V(J)$ and $D(J) \subset D(I)$. The **distinguished open sets**

$$D(f) = \{\mathfrak{p} \in \mathrm{Spec}(R) : f \notin \mathfrak{p}\}$$

for $f \in R$ therefore form a base for the Zariski topology, so that every Zariski open is a union of distinguished opens.

Exercise II.3.1 Show that the closed points of $\mathrm{Spec}(R)$ are precisely the maximal ideals of R.

Exercise II.3.2 Show the Zariski topology is always **quasicompact** (i.e. every open cover has a finite subcover) and T_1 but is typically non-Hausdorff, and thus typically not compact (because compact iff it is quasicompact and Hausdorff by Heine-Borel).

Exercise II.3.3 Show the Zariski topology is the coarsest T_1 topology on $\mathrm{Spec}(R)$.

II.3.1 Localization

A **localization** of a commutative ring R by a subset $S \subset R$ is an R-algebra isomorphic to $R[S^{-1}]$. The subset is called **multiplicatively closed** if S is multiplicative monoid, in which case $R[S^{-1}] = S^{-1}R$. In general we have $R[S^{-1}] = \langle S \rangle^{-1}R$, where $\langle S \rangle$ is the monoid generated by the elements of S. Examples include localization $R[f^{-1}]$ by a principal ideal $(f) = Rf$ and localization $R_{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1}R$ at a prime ideal $\mathfrak{p}$. Modules can be localized via the tensor product $S^{-1}M = M \otimes_R (S^{-1}R)$. Furthermore,

$$\mathrm{Spec}(S^{-1}R) \simeq \{\mathfrak{p} : \mathfrak{p} \cap S = \emptyset\} \subset \mathrm{Spec}(R).$$

II.3.2 Spec(R) as a locally ringed space

There is a canonical sheaf $\mathcal{O}_{\mathrm{Spec}(R)}$ of rings on $\mathrm{Spec}(R)$ such that

$$\mathcal{O}_{\mathrm{Spec}(R)}(D(f)) \simeq R[f^{-1}] = \bigcap_{f \notin \mathfrak{p}} R_{\mathfrak{p}}$$

for each nonzero $f \in R$. The stalks are local rings

$$\mathcal{O}_{\mathrm{Spec}(R)}(\mathfrak{p}) = R_{\mathfrak{p}} = (S \setminus \mathfrak{p})^{-1}R$$

so $(\mathrm{Spec}(R), \mathcal{O}_{\mathrm{Spec}(R)})$ is a locally ringed space. Furthermore,

$$\mathcal{O}_{\mathrm{Spec}(R)}(U) = \bigcap_{\mathfrak{p} \in U} \mathcal{O}_{\mathrm{Spec}(R)}(\mathfrak{p}).$$

The inclusion map $R \to R[f^{-1}]$ is dual to the inclusion

$$\mathrm{Spec}(R[f^{-1}]) \hookrightarrow \mathrm{Spec}(R)$$

with image $D(f)$ and the quotient map $R \to R/I$ is dual to the open mapping

$$\mathrm{Spec}(R/I) \to \mathrm{Spec}(R)$$

with image $V(I)$. These are our first examples of **finite morphisms**.

II.3.3 Commutative Noetherian rings

An ideal Q of R is **primary** if $xy \in Q$ implies either $x \in Q$, $y \in Q$ or $x, y \in \sqrt{Q}$. An ideal Q is primary iff every zero divisor in R/Q is nilpotent.

Lasker-Noether Theorem. Every ideal of a commutative Noetherian ring has an irredundant primary decomposition

$$Q_1 \cap \cdots \cap Q_m$$

with distinct uniquely determined prime radicals $\sqrt{Q_i}$ though the primary ideals Q_i can in general be different.

Examples from [17].

II.3.4 Integral domains

An **integral domain** is a commutative ring R with no zero divisors, i.e. a commutative domain. A commutative ring R is an integral domain iff $(0) \in \mathrm{Spec}(R)$ i.e. (0) is a prime ideal. In such a case, the localization $R_{(0)}$ is the fraction field $\mathrm{Frac}(R)$. Localizations of integral domains are integral domains.

An ideal $I \subset R$ is prime iff R/I is an integral domain and maximal iff R/I is a field. Because fields are integral domains, every maximal ideal is prime, but there can be non-maximal prime ideals in general. Example: Every prime of the Dedekind domain $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ is maximal but the a non-integrally closed Noetherian domain like $\mathbb{Z}[\sqrt{5}]$ can have non-maximal prime ideals (in this case, there is a prime strictly dividing 2).

Examples of integral domains and their fraction fields include

$$\mathbb{Z} \subset \mathbb{Q}, \quad \mathbb{Z}\left[\frac{1}{n}\right] \subset \mathbb{Q}, \quad \mathbb{Z}_{(n)} \subset \mathbb{Q}, \quad \mathbb{Z}_p \subset \mathbb{Q}_p.$$

II.4 Schemes

II.4.1 Categories of schemes

An **affine scheme** is a locally ringed space isomorphic to some $\mathrm{Spec}(R)$. An affine scheme X is **reduced** if $\mathcal{O}_X$ is reduced, **irreducible** if its underlying topological space is, and **integral** if $\mathcal{O}_X$ is an integral domain.

A **scheme** is a locally ringed space covered by affine schemes. A scheme is **reduced**, **irreducible** or **integral** if that property holds on all its affine opens. Reduced and integral can also be checked at the level of local rings. A **morphism** $X \to Y$ of schemes is a morphism of the underlying locally ringed spaces.

A scheme X equipped with a **structure morphism** $X \to Z$ to a **base scheme** Z (written X/Z) is called a **Z-scheme**, a scheme **over** Z, or a scheme **defined over** Z. If furthermore $Z = \mathrm{Spec}(R)$ is affine we may say that X is defined over R.

A morphism of schemes over Z is a morphism $f : X \to Y$ that commutes with the structure maps, sometimes written $f : X/Z \to Y/Z$. The **cartesian**, or **fiber product** $X \times_Z Y$ in the resulting category Sch_Z of Z-schemes exists and satisfies the usual universal properties for products.

II.4.2 Separated morphisms and varieties

A morphism $f : X \to Y$ is a **closed immersion** if $f^\sharp : \mathcal{O}_Y \to f_*\mathcal{O}_X$ is surjective. A morphism $f : X \to Z$ is **separated** if the diagonal morphism $\delta : X \to X \times_Z X$ is a closed immersion, i.e. $\delta^\sharp : \mathcal{O}_{X\times_Z X} \to f_*\mathcal{O}_X$ is surjective. In such a case, the relative scheme X/Z is also said to be separated.

Exercise II.4.1 Let $I \subset R$ is an ideal. Show that the inclusion $\mathrm{Spec}(R/I) \to \mathrm{Spec}(R)$ defined by the quotient map $R \to R/I$ is a closed immersion.

A **variety** usually at least means a reduced, separated scheme of finite type over a field. Many authors further require irreducibility (hence integrality) and/or algebraic closedness of the base field.

II.4.3 Affine algebras

If S is an R-algebra, the defining morphism $R \to S$ determines a structure morphism $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ of affine schemes, defining $\mathrm{Spec}(S)$ over R (i.e. as a **relative scheme** over $\mathrm{Spec}(R)$). If S is finitely generated over R, then $\mathrm{Spec}(S)$ is of **finite type** (or just **finite**) over R.

If S is reduced and finite over R, then $\mathrm{Spec}(S)$ is an **affine algebraic set** that is irreducible iff S is furthermore an integral domain. Typically an **affine algebraic variety** refers to an irreducible affine algebraic set over an algebraically closed field though this terminology is not universal with some authors dropping the irreducibility and the base field condition.

There is an equivalence of categories between the category of finite reduced R-algebras and homomorphisms and the category of affine algebraic sets and finite morphisms.

The image of an affine algebraic set in **affine space** $\mathbb{A}^m_R = \mathrm{Spec}(R[x_1, \ldots, x_m])$ over R is $\mathrm{Spec}(R[x_1, \ldots, x_m]/I)$ for some radical ideal $I = \sqrt{I}$ that is prime for a variety.

For a field K, $\mathrm{Spec}(K)$ consists of the single point (0) so its sheaf is given by the stalk $\mathcal{O}_{(0)} = K$.

Nullstellensatz $\sqrt{J} = I(V(J))$ characterizes the closed sets in the Zariski topology. Noether normalization.

The **functor of points** takes each commutative R-algebra S to the set $\mathrm{Spec}(S)(T)$ of **T-valued points** $\mathrm{Spec}(T) \to \mathrm{Spec}(S)$, which are represented by R-algebra homomorphisms $S \to T$. If k is a field and K/k is an extension, the K-valued points are

k-algebra homomorphisms $S \to K$. If the extension K/k is normal and separable, the $\mathrm{Gal}(K/k)$-orbits of the K-valued points are in natural bijection with the maximal points of $\mathrm{Spec}(S)$.

$\mathrm{Spec}(\mathbb{Z})$ consists of a closed point (p) for each finite prime p together with the nonmaximal prime (0) with $\overline{(0)} = \mathrm{Spec}(\mathbb{Z})$.

II.4.4 Dimension and rank

The **Krull dimension** of a commutative ring R is the dimension of $\mathrm{Spec}(R)$ as a topological space. It is equal to the length of the longest chain of prime ideals, measured by the number of inclusions. For example, $\mathbb{Q}(\sqrt{-3})$ has dimension 0 (as do all fields), $\mathbb{Z}$, $\mathbb{Z}\left[\sqrt{-3}\right]$ and $\mathbb{C}[x]$ have dimension 1, whereas $\mathbb{C}[x, y]$ and $\mathbb{Z}[x]$ have dimension 2.

The **rank** of a finitely generated projective module M over a commutative ring R is the following locally constant function on $\mathrm{Spec}(R)$:

$$\mathfrak{p} \mapsto \mathrm{rank}_{\mathfrak{p}}(M) = \mathrm{rank}_{R/\mathfrak{p}}(M \otimes_R R/\mathfrak{p}).$$

It is well-defined because $M \otimes_R R/\mathfrak{p}$ is free over the local ring $R/\mathfrak{p}$. When $\mathrm{Spec}(R)$ is connected, R is an integral domain and 1 is the only nontrivial idempotent. If F is the quotient field of R, then

$$\mathrm{rank}(M) = \dim_F(F \otimes_R M) = \text{ maximum number of linearly independent elements in } M.$$

II.4.5 Dedekind domains

An integral domain R that is not a field is a **Dedekind domain** if it satisfies any of the following equivalent conditions:

- Every nonzero proper ideal of R uniquely factors into prime ideals.
- Every nonzero fractional ideal of R is invertible.
- R is Noetherian and its localization $R_{\mathfrak{m}}$ at each maximal ideal $\mathfrak{m}$ is a DVR.
- R is 1-dimensional (so every prime ideal is maximal), Noetherian and integrally closed.
- Every submodule of every projective R-module is projective.

The orders of a number field K are standard examples of one-dimensional Noetherian domains and, among these, only the maximal order (i.e. the ring of integers) is integrally closed, hence a Dedekind domain.

The class of Dedekind domains is closed under localization: If R is a Dedekind domain and $S \subset R$ is multiplicatively closed, then the localization $S^{-1}R$ is also a Dedekind

domain that is not R-integral. So for example, $\mathbb{Z}$, $\mathbb{Z}[\frac{1}{p}]$ and $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$ are all Dedekind domains. Dedekind domains are also closed under extension: If R is a Dedekind domain with quotient field F, and if E/F is any extension field, then the integral closure of R in E is a Dedekind domain with quotient field E. For example, the p-adic integers $\mathbb{Z}_p$ are the integral closure of $\mathbb{Z}_{(p)}$ (in fact, also of $\mathbb{Z}$) in the p-adic numbers $\mathbb{Q}_p/\mathbb{Q}$, hence a Dedekind domain.

Exercise II.4.2 What goes wrong for $\mathbb{Z}[\sqrt{-3}]$?

II.4.6 Modules over commutative rings

In this section we consider only modules over a commutative ring R. A module is **flat** if it preserves exact sequences under tensor products, and **faithfully flat** when the tensor product with a sequence is exact iff the original sequence is exact. A module M is **torsion free** if the annihilator of any nonzero element of M contains only zero divisors, i.e. if $rm = 0$ implies that m is a zero divisor. Over a domain, torsion free $\Rightarrow$ faithful since the condition becomes $rm = 0$ implies $m = 0$.

We have the general implications

$$\text{free} \Rightarrow \text{projective} \Rightarrow \text{flat} \Rightarrow \text{torsion-free}.$$

It is worth mentioning that the proof of free $\Rightarrow$ projective uses the axiom of choice whereas one can prove free $\Rightarrow$ flat without it.

For modules over a PID, projective $\Rightarrow$ free.

Let M be a finitely generated module over a commutative ring R. Then M is a

If R is a local ring, then M is flat $\Rightarrow$ M is free.

For finitely generated modules over Dedekind domain, torsion-free $\Rightarrow$ projective.

For finitely generated modules over a PID, torsion-free $\Rightarrow$ free.

For finitely generated modules over an integrally closed Noetherian domain, flat $\Rightarrow$ projective.

Quasicoherent sheaves, locally free and coherent sheaves on $\mathrm{Spec}(R)$ are R-modules, projective R-modules and finitely presented R-modules.

II.5 Projective schemes

In this section, graded means $\mathbb{Z}$-graded unless stated otherwise.

II.5.1 Proj(R)

A homogeneous ideal I of a graded ring R is **irrelevant** if its radical $\sqrt{I}$ contains the **irrelevant ideal** R_+. Let $\mathrm{Proj}(R)$ be the set of relevant homogeneous prime ideals of R, i.e. the homogeneous prime ideals that are strictly contained in S_+. The relevant homogeneous ideals I determine the Zariski-closed

$$V(I) = \{\mathfrak{p} \in \mathrm{Proj}(R) : \mathfrak{p} \supset I\}$$

and Zariski-open

$$D(I) = \mathrm{Proj}(R) \setminus V(I) = \{\mathfrak{p} \in \mathrm{Proj}(R) : \mathfrak{p} \supset I\}$$

subsets. The homogenous $f \in R_+$ define the **distinguished closed**

$$V(f) = V((f)) = \{\mathfrak{p} \in \mathrm{Proj}(R) : \mathfrak{p} \ni f\}$$

and **distinguished open**

$$D(f) := \mathrm{Proj}(R) \setminus V(f) = \{\mathfrak{p} \in \mathrm{Proj}(R) : \mathfrak{p} \not\ni f\}$$

subsets.

II.5.2 On homogeneous ideals

We record here some useful facts about graded rings and their homogeneous ideals following [18]. Let R be a graded ring. Then R_0 is a ring and R is an R_0-algebra. If S is a multiplicative subset of R, let $\mathcal{I}(S)$ be the set of homogeneous ideals I with $I \cap S = \emptyset$. Then the maximal ideals of $\mathcal{I}(S)$ are prime, and every ideal of $\mathcal{I}(S)$ is contained in a prime of $\mathcal{I}(S)$. If R a domain, then only homogeneous elements can divide homogeneous elements.

A homogeneous subset of R_+ generates R as an R_0-module iff it generates R_+ as an R-module. The ideal $R_+ \subset R$ is finitely generated iff R is a finitely generated R_0-algebra. R is Noetherian iff R_0 is Noetherian and R is a finitely generated R_0-algebra. Let $R^{(d)}$ be the graded ring with $R^{(d)}_n = R_{nd}$. If it is generated by R_1 as an R_0-algebra, then so is every $R^{(d)}$ by $R^{(d)}_1 = R_d$ (similarly for "finitely generated by"). If R is Noetherian, then so is $R^{(d)}$. If R is a finitely generated R_0-algebra, then so is $R^{(d)}$ for some d.

For a homogeneous ideal $\mathfrak{a} \subset R$ and $\mathfrak{p} \in \mathrm{Proj}(R)$, then $\mathfrak{a} \subset \mathfrak{p}$ iff $\mathfrak{a}_n \subset \mathfrak{p}_n$ for all sufficiently large n.

Let $\mathfrak{p}_n \subset R_n$ for all $n \geq N$ be subgroups satisfying the following conditions: $\mathfrak{p}_n \neq S_n$ for some $n \geq d$. $R_m\mathfrak{p}_n \subset \mathfrak{p}_{n+m}$ for all $m \geq 0$, $n \geq N$. For all $m \geq 0$, $f \in R_n$ and $g \in R_{n'}$ with $n, n' \geq N$, $fg \in \mathfrak{p}_{n+n'} \Rightarrow f \in \mathfrak{p}_n$ or $g \in \mathfrak{p}_{n'}$. Then it completes to a unique $\mathfrak{p} \in \mathrm{Proj}(R)$.

If $f \in R_d$, then $R_{(f)}$ and $R^{(d)}/(f-1)$ canonically isomorphic.

II.5.3 Proj(R) as a scheme

For each homogeneous $f \in R_+$, there is an isomorphism $D(f) \to \mathrm{Spec}(R[f^{-1}]_0)$ taking $\mathfrak{p} \in D(f)$ to $(R[f^{-1}]\mathfrak{p})_0$ and $\mathfrak{q} \in \mathrm{Spec}(R[f^{-1}]_0)$ to $\mathfrak{q} \cap R$, as can be verified by showing bijections with the homogeneous primes of $R[f^{-1}]$. The distinguished opens form a base for the Zariski topology (every open is a union of $D(f)$), so that for every open $U \subset \mathrm{Proj}(R)$, there is a set $\{f_i\}$ of homogeneous elements such that

$$\mathcal{O}(U) \simeq S[\{f_i^{-1}\}]_0 = R\left[\prod_i f_i^{-1}\right]_0,$$

with the last holding if e.g. R is Noetherian, in which case the ideal of U must be finitely generated. A set of basic opens $D(f_i)$ cover $\mathrm{Proj}(R)$ iff the radical of the ideal generated by the f_i is R_+ (Eisenbud Exercise III-10).

The structure sheaf has stalks

$$\mathcal{O}_\mathfrak{p} := \lim_{U \ni \mathfrak{p}} \mathcal{O}(U) \simeq R_\mathfrak{p} = R[(R\backslash\mathfrak{p})^{-1}]_0 = \{g/f : g, f \text{ homog. of same degree, } f \notin \mathfrak{p}\} = \bigcap_{f \notin \mathfrak{p}} R[f^{-1}]_0$$

The closed points of $\mathrm{Proj}(R)$ are the maximal ideals among those in $\mathrm{Proj}(R)$; equivalently, they are the maximal homogeneous ideals of S among those strictly contained in R_+. Note that points of $\mathrm{Proj}(R)$ are never maximal ideals of R, because they are all contained in R_+. The Proj construction remedies this by ignoring the irrelevant ideal, but this means that $R/\mathfrak{p}$ is an integral domain but not a field for each $\mathfrak{p} \in \mathrm{Proj}(R)$.

If $f \in S_1$, then $R[f^{-1}]_{-n} = S[f^{-1}]_0/f^n$ for $n \geq 0$. If $\mathfrak{p} \in \mathrm{Proj}(R)$ and $f \notin \mathfrak{p}$, the prime ideal $(R[f^{-1}]\mathfrak{p})_0$ of $R[f^{-1}]_0$ has the form

$$(R[f^{-1}]\mathfrak{p})_0 \;=\; S[f^{-1}]_0\mathfrak{p}_0 + R[f^{-1}]_{-1}\mathfrak{p}_1 + \cdots = R[f^{-1}]_0(\mathfrak{p}_0 + \mathfrak{p}_1/f + \mathfrak{p}_2/f^2 + \cdots).$$

A similar formula exists for $f \in R_m$. In either case, the ideal $(R[f^{-1}]\mathfrak{p})_0$ is maximal iff $\mathfrak{p}$ is a closed point, in which case the residue field $k(\mathfrak{p}) = R[f^{-1}]_0/(R[f^{-1}]\mathfrak{p})_0$ is independent, up to isomophism, of the choice of $f \notin \mathfrak{p}$.

If F/k is a field extension, the set of F-valued points of $\mathrm{Proj}(R)$, or of F-points, is defined to be

$$\mathrm{Proj}(S)(F) := \mathrm{Hom}(\mathrm{Spec}(F), \mathrm{Proj}(S)).$$

A morphism $\mathrm{Spec}(F) \to \mathrm{Proj}(R)$ determines a morphism $\mathcal{O}_{\mathrm{Proj}(R)} \to \pi^*\mathcal{O}_{\mathrm{Spec}(F)}$ of sheaves over $\mathrm{Proj}(S)$, which by adjointness, is equivalent to a morphism $\pi^{-1}\mathcal{O}_{\mathrm{Proj}(R)} \to \mathcal{O}_{\mathrm{Spec}(F)}$of sheaves over the 1-point space $\mathrm{Spec}(F)$. Hence, to give an F-point is to give a closed point $\mathfrak{p}$ and a k-algebra homomorphism $R[f^{-1}]_0 \to F$ for every $f \notin \mathfrak{p}$. Because the kernel of this homomorphism is the maximal ideal $(R[f^{-1}]_0\mathfrak{p})$ (why?), F-valued points are also equivalent to a choice of closed point $\mathfrak{p}$ together with an embedding $k(\mathfrak{p}) \to F$.

The residue field $k(\mathfrak{p})$ is a finite extension of k iff $\mathfrak{p}$ is a closed point iff the degree $[k(\mathfrak{p}) : k]$ is finite. The closed points are in 1-1 correspondence with the space

$\mathrm{Proj}(R)(\bar{k})/\mathrm{Gal}(\bar{k}/k)$ of Galois orbits of $\bar{k}$-points. There is a 1-1 correspondence between F-points and closed points equipped with embeddings $k(\mathfrak{p}) \to F$ of their residue fields.

[[15] Exercise 4.5.I]: For a homogeneous ideal $I \subset R$, $V(I) = \emptyset$ iff $S_+ \subset \sqrt{I}$ iff for a set of generators f_i of I, $\cup_i D(f_i) = \mathrm{Proj}(R)$. So to show that $V(I) \neq \emptyset$ for $I = RH_2^G$, it is enough to show that $R_+ \not\subset \sqrt{I}$, i.e. to show that $f^n \in RH_2^G \Rightarrow f_0 \neq 0$.

If $I \subset R$ is a relevant homogeneous ideal, its **saturation** is the ideal

$$I^{\mathrm{sat}} = \{f \in R : fR_n \subset I \text{ for some } n\} = \bigcup_n (I : S_+^n),$$

where $(I : J) = \{f \in R : fJ \subset I\}$ is the ideal quotient. There is a 1-1 correspondence between saturated ideals of R and projective subschemes of $\mathrm{Proj}(R)$. Note that the **radical** of an ideal $I \subset R$ is the ideal

$$\sqrt{I} = \{f \in R : f^n \in I \text{ for some } n\} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p},$$

and that the intersection can be restricted to homogeneous primes if I is homogeneous.

Chapter III
Quadratic forms

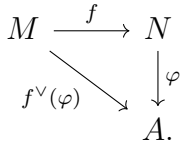
We discuss involutions, sesquilinear forms, tensor products, bimodules and Morita equivalence, following [5], [19].

III.1 The dual module

Let M be a module over a ring A. The **dual module** $M^\vee = \mathrm{Hom}(M, A)$ is the right module with action $(\varphi a)(x) = \varphi(ax)$. This construction extends to a duality functor, i.e an anti-equivalence

$$\vee \colon A\text{−}\mathsf{mod} \to \mathsf{mod}\text{−}A$$

of categories taking f to its **transpose** $f^\vee \colon N^\vee \to M^\vee$, which maps each $\varphi \in \mathrm{Hom}(N, A)$ to its **pullback** $f^\vee(\varphi) = \varphi \circ f$ along f in the diagram



III.2 Involutions

An **involution** $\iota : A \to A$ on a ring A is an anti-automorphism squaring to the identity. Composing with the natural anti-isomorphism $A^{\mathrm{op}} \to A$ gives a bijection between the involutions on A and the isomorphisms $A \to A^{\mathrm{op}}$. Each involution defines a corresponding **norm** $N(a) = a\iota(a)$ and a **trace** $\mathrm{Tr}(a) = a + \iota(a)$.

Let (A, ι) be a ring with involution. If A is noncommutative, then ι must be nontrivial. It a nontrivial fact that a given ring admits an involution at all. Involutions relate left and right modules while underlying the definitions of affine algebraic groups.

Let R be a commutative subring of A. Viewed as an R-algebra, an involution on A is of the **first kind** if it acts trivially on R and is otherwise of the **second kind**, restricting to a nontrivial automorphism of R.

III.3 The opposite module and its dual

Given an A-module, we may use the involution to define the **opposite module** $\overline{M}$, a right module with same underlying abelian group but with right action $ma = \iota(a)m$. This construction extends to an equivalence of categories $A\text{−}\mathsf{mod} \to \mathsf{mod}\text{−}A$ taking

$f\colon M \to N$ to the morphism $\overline{f}\colon \overline{M} \to \overline{N}$ with $\overline{f}(m) = f(m)$. With similar definitions for right modules, the functors $\cdot^\vee$ and $\overline{\ }$ commute up natural isomorphism (see [5] Lemma 2.1.1). Their composition is a duality functor $* : A\text{−}\mathsf{mod} \to A\text{−}\mathsf{mod}$ such that $M^* := \overline{M^\vee}$ via $(af)(x) = f(x\bar{a})$, mapping $f : M \to N$ to its transpose $f^* = f^\vee : N^* \to M^*$, which takes $\varphi \in N^*$ to $\varphi \circ f \in M^*$. There are natural isomorphisms $\overline{\ }^\vee \simeq \overline{\ }^\vee$ and $** \simeq \mathrm{id}_{A\text{−}\mathsf{mod}}$ [19].

III.4 Sesquilinear forms

Here we recall some general background [5], [19] enabling the realization of quadratic forms as classes of bilinear forms modulo alternating ones that works in any characteristic, most notably 2.

Let A/R be an involuted algebra and let M be a right A-module. A bi-additive map $b : M \times M \to A$ is a **sesquilinear form** if $b(xa, ya') = \bar{a}b(x, y)a'$ for every $x, y \in M$ and every $a, a' \in A$. Each sesquilinear form $b \in \mathrm{Sesq}(M)$ defines a unique **adjoint** morphism $h_b \in \mathrm{Hom}_A(M, M^*)$ such that $h_b(x)(y) = b(x, y)$ for all $x, y \in M$, inducing the R-module isomorphisms

$$\mathrm{Sesq}(M) \simeq \mathrm{Hom}_A(M, M^*) \simeq M \otimes_A \overline{M}.$$

Call a sesquilinear form b **regular**, **nonsingular**, or **nondegenerate** if its adjoint $h_b \in \mathrm{Hom}_A(M, M^*)$ is an isomorphism. When b is regular, the **adjoint involution** $f \mapsto f^b := h_b^{-1} f^* h_b$ on $\mathrm{End}_A(M)$ is the unique involution such that $b(x, fy) = b(f^b x, y)$ for every $x, y \in M$.

Let $\bar{b}(x, y) = \overline{b(y, x)}$. For $\varepsilon \in \mathrm{U}_1(Z(A)) := \{\varepsilon \in Z(A) : \varepsilon\bar{\varepsilon} = 1\} \subset A^\times$, define $S_\varepsilon : \mathrm{Sesq}(M) \to \mathrm{Sesq}(M)$ by $S_\varepsilon(b) = b + \varepsilon\bar{b}$ and similarly define

$$S_\varepsilon : \mathrm{Hom}_A(M, M^*) \to \mathrm{Hom}_A(M, M^*).$$

Let

$$\mathrm{Sesq}^\varepsilon(M) = \{b \in \mathrm{Sesq}(M) : \bar{b} = \varepsilon b\}$$

be the R-submodule of **ε-hermitian** forms on M. 1-hermitian forms are **hermitian** and -1-hermitian forms **antihermitian**.

III.5 Form rings

Let

$$\mathrm{Sesq}_\varepsilon(M) = \{S_\varepsilon(b) : b \in \mathrm{Sesq}(M)\} \subset \mathrm{Sesq}^\varepsilon(M)$$

be the submodule of **even** ε-hermitian forms. There is an exact sequence

$$0 \to \mathrm{Sesq}^{-\varepsilon}(M) \longrightarrow \mathrm{Sesq}(M) \xrightarrow{S_\varepsilon} \mathrm{Sesq}_\varepsilon(M) \to 0.$$

Let $S^\varepsilon = \ker S_{-\varepsilon}$ and define

$$\Lambda_{\min} = S_{-\varepsilon}(A) = \{a - \varepsilon\bar{a}\},\ \ \Lambda_{\max} = S^{-\varepsilon}(A) = \{a : a = -\varepsilon\bar{a}\}.$$

Each intermediate additive subgroup $S_{-\varepsilon}(A) \subset \Lambda \subset S^{-\varepsilon}(A)$ satisfying $a\Lambda\bar{a} \subset \Lambda$ (note that $S_{-\varepsilon} = S^{-\varepsilon}$ when $2 \in A^\times$) determines a **form ring** [10], [19], or **unitary ring** [6], $(A, \varepsilon, \Lambda)$ with **form parameter** (ε, Λ).

An ε-hermitian form b on a finitely generated projective right A-module M determines an **ε-hermitian module** (M, b). [19] calls a pair (M, B) with $B \in \mathrm{Sesq}(M)$ a **Λ-quadratic module** and the map $q_B : M \to A/\Lambda$ taking m to $B(m, m) + \Lambda$ a **Λ-quadratic form**.

The book [10] studies codes over a right A-module M as submodules of the product module M^n. They approach the notion of a form ring and form parameter in a different but equivalent way through the following definitions:

A function $\phi : M \to N$ between right A-modules is a **quadratic map** if

$$\phi(x, y) := \phi(x + y) - \phi(x) - \phi(y) + \phi(0)$$

is biadditive. It **homogeneous** if it is **pointed** ($\phi(0) = 0$) and **even** ($\phi(-x) = \phi(x)$), or equivalently if $\phi(nx) = n^2\phi(x)$ for every $n \in \mathbb{Z}$. A **quadratic form** is a homogeneous quadratic map.

An **A-qmodule** is an abelian group Φ together with a pointed quadratic map $[\cdot] : A \to \mathrm{End}(\Phi)$ such that $[1] = 1$ and $[rs] = [r][s]$. A **twisted A-module** is a right $(A \times A)$-module M equipped with an automorphism τ satisfying $\tau(m(r \otimes s)) = \tau(m)(s \otimes r)$. A **twisted ring** is a ring A together with a twisted A-module M and a right A-module isomorphism $\psi : A_A \to M_{1\otimes A}$ such that $\varepsilon := \psi^{-1}(\tau(\psi(1))) \in A^\times$.

Finally, they define a form ring (A, M, ψ, Φ) as a twisted ring (A, M, ψ) equipped with an A-qmodule isomophism $M \to \Phi$. They call the isomorphic A-qmodules M and Φ a "quadratic pair" but this means something else in [2].

Exercise III.5.1 Show that a twisted ring (A, M, ψ) is the same as a ring with involution induced by τ and ψ, in which case M is an A-qmodule for the diagonal action $m[r] = m(r \otimes r)$. (see [10] Sect. 1.4).

III.6 Determinant and discriminant of hermitian forms

Let $h\colon M \times M \to R$ be a nondegenerate hermitian form on a module M over a commutative ring R with involution ι. If M is a free module of rank r, define the **determinant** of h to be the determinant of the Gram matrix of any basis $e_1, \ldots, e_r$ modulo norms

$$\det(h) = \det(h(e_i, e_j)_{ij})\,\mathrm{N}(R^\times) \in R^\times/\,\mathrm{N}(R^\times),$$

where $\mathrm{N}(x) = x\iota(x)$ is the **norm** induced by the involution ι. The **discriminant** of h is the class of the signed determinant

$$\mathrm{disc}(h) = (-1)^{(r^2-r)/2} \det(h) \in R^\times / \mathrm{N}(R^\times).$$

When the involution ι is trivial, note that $\mathrm{N}(R^\times) = (R^\times)^2$ and we recover the usual notion of discriminant being defined modulo squares of the base ring.

If M is an R-module of constant rank r, define $\mathrm{disc}(h)$ to be the ideal of R generated by the determinants $\det(h(e_i, e_j)_{ij})$ of the Gram matrices of all linear independent subsets $\{e_1, \ldots, e_r\} \subset M$. If R is an integral domain, this is the ideal generated by the determinants of all R-sublattices of M.

III.7 Quadratic lattices

Let R be a commutative ring and let M and N be R-modules. A function $q\colon M \to N$ is a **quadratic form** if

$$B_q(x, y) := q(x + y) - q(x) - q(y)$$

is a symmetric bilinear form and $q(rx) = r^2 q(x)$ for every $r \in R$ and every $x \in M$. When q is R-valued, we call (M, q) a **quadratic R-module**. A quadratic module that is also an **R-lattice** (i.e. a finite-rank torsion-free module over an integral domain R that is not a field) is a **quadratic R-lattice**. A quadratic module over a field is a **quadratic space**, and every quadratic R-lattice (L, q) embeds naturally into its ambient quadratic space (L_K, q), where K is the quotient field of R and $L_K = K \otimes_R L$.

An **isometry** $W\colon (M', q') \to (M, q)$ of quadratic R-modules is an injective R-linear map $W\colon M' \to M$ such that $q' = q \circ W$. We write $M' \simeq M$ when the modules are **isomorphic**, meaning there exists a surjective isometry, or equivalently, a pair of isometries $M' \to M$ and $M \to M'$. Denote the **automorphism group** $\mathrm{O}(M) = \mathrm{Isom}(M, M)$. Note that for every commutative ring S containing R, there are natural embeddings $\mathrm{Isom}(M', M) \hookrightarrow \mathrm{Isom}(M'_S, M_S)$ and $\mathrm{O}(M) \hookrightarrow \mathrm{O}(M_S)$. Two R-lattices L and L' in a common quadratic space V/K are **properly isomorphic** if $L' = g(L)$ for some $g \in \mathrm{SO}(V)$. Then $\mathrm{SO}(L) = \mathrm{O}(L) \cap \mathrm{SO}(L_F)$ is the subgroup of proper automorphisms. A lattice L is **ambiguous** if $\mathrm{SO}(L) \neq \mathrm{O}(L)$, i.e. if it possesses an improper automorphism.

Let $K, K' \in F^{n\times n}$ be matrices. An R-linear map $W\colon R^n \to R^n$ between free quadratic R-lattices (R^n, K') and (R^n, K) is just a matrix in $R^{n\times n}$. Such a W is an isometry if $K' = W^T K W$ and it is an isomorphism if also $W \in \mathrm{GL}_n(R)$, in which case $W(R^n, K') = (R^n, W^{-T} K' W^{-1}) = (R^n, K)$. Note that if we are given an extension ring $R \subset S$, an isometry $L'_S \to L_S$ of the corresponding quadratic S-lattices is now simply an S-linear map $W\colon S^n \to S^n$ for which $K' = W^T K W$ as before.

Every bilinear form $B\colon M \times M \to N$ determines an R-linear map $B^\vee\colon x \mapsto B(x, \cdot)$ from M to $\mathrm{Hom}_R(M, N)$. Call B **nondegenerate** if $B^\vee$ is injective, i.e. if $B(x, y) = 0$

for every $y \in M$ implies that $x = 0$. If $B^\vee$ is an isomorphism, then B is **regular** (or **nonsingular**, or a **pairing**). A quadratic form q is nondegenerate if B_q is nondegenerate, nonsingular if B_q is nonsingular, and **unimodular** if B_q is a pairing. Note that all three notions coincide when M is a vector space and N is the underlying field. (Not 100 percent sure of these definitions).

Call a quadratic lattice (L, q) **classically integral** if $B_q(L, L) \subset 2R$, in which case $q(x, y) := \frac{1}{2}B_q(x, y)$ is a integral symmetric bilinear form with $q(x, x) = q(x)$. A quadratic lattice (L, q) is **even** if $q(L) \subset 2R$ and otherwise it is **odd**. Every even lattice is classically integral but there are odd lattices that are not classically integral.

A quadratic R-lattice (Λ, q) naturally embeds into its **dual**

$$\Lambda^* = \{y \in \Lambda_{\mathbb{Q}} : B_q(\Lambda, y) \subset R\} \simeq \mathrm{Hom}(\Lambda, R),$$

and induces a finite quadratic form $\bar{q}\colon \Lambda^*/\Lambda \to \mathbb{Q}/\mathbb{Z}$ on the **discriminant group** Λ^*/Λ.

If (Λ, q) is classically integral, then Λ embeds into its **classical dual**

$$\Lambda^\# := \{y \in \Lambda_{\mathbb{Q}} : q(\Lambda, y) \subset R\} = \{y \in \Lambda_{\mathbb{Q}} : B_q(\Lambda, y) \subset 2R\} \simeq \mathrm{Hom}(\Lambda, 2R),$$

which satisfies $\Lambda^\# = 2\Lambda^*$ and $\Lambda \subset \Lambda^\# \subset \Lambda^*$. The finite quadratic form $\bar{q}$ restricts to $\Lambda^\#/\Lambda$ and the induced bilinear form $\bar{b}_q\colon \Lambda^\#/\Lambda \times \Lambda^\#/\Lambda \to \mathbb{Q}/\mathbb{Z}$ satisfies $\bar{q}([x]) = \bar{b}_q([x], [x])$.

If Λ is even, then we may also define $\tilde{q}\colon \Lambda^*/\Lambda \to \mathbb{Q}/2\mathbb{Z}$ via $\tilde{q}([x]) = q(x) + 2\mathbb{Z}$ so that the following diagram commutes:

$$\begin{array}{ccc} & & \mathbb{Q}/2\mathbb{Z} \\ & \nearrow & \big\downarrow{\scriptstyle \mathrm{mod}\ 1} \\ \Lambda^*/\Lambda_{\tilde{q}}^{\tilde{q}} & \longrightarrow & \mathbb{Q}/\mathbb{Z}. \end{array}$$

For all $x, y \in \Lambda^\#$, it satisfies

$$\bar{b}_q([x], [y]) = \frac{1}{2}\big(\tilde{q}([x] + [y]) - \tilde{q}([x]) - \tilde{q}([y])\big),$$

while $e^{\pi i \tilde{q}([x])}$ is a canonical square root of $e^{2\pi i \bar{q}([x])} = e^{2\pi i \bar{b}_q([x],[x])}$ on $\Lambda^\#/\Lambda$. In this case, we obtain a projective representation of $\mathrm{SL}_2(\mathbb{Z})$ for which $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \mapsto S$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \mapsto T$, where

$$S_{[x],[y]} = \frac{1}{\tau(\tilde{q})} e^{2\pi i \bar{b}_q([x],[y])}, \quad T_{[x],[x]} = e^{\pi i \tilde{q}([x])} = e^{\pi i q(x)},$$

where

$$\tau(\tilde{q}) = \sum_{[x]} e^{\pi i \tilde{q}([x])} = \sqrt{|\Lambda^\#/\Lambda|}\, e^{2\pi i \sigma/8}$$

is a Gauss sum and σ is the signature. When $\mathrm{rank}(\Lambda)$ is even, this is a linear representation of $\mathrm{SL}_2(\mathbb{Z})$ and when $\mathrm{rank}(\Lambda)$ is odd, it lifts to a linear representation of the metaplectic double cover $\widetilde{\mathrm{SL}}_2(\mathbb{Z})$.

If Λ is an odd classically integral lattice, a **characteristic vector** for Λ is any $c \in \Lambda^\#$ such that $c \cdot x \equiv x \cdot x \bmod 2$ for every $x \in \Lambda$, i.e. such that $\{x \in \Lambda : x \cdot c \equiv 0 \bmod 2\}$ is the index-2 even sublattice.

$\mathbb{Q}/\mathbb{Z}$ and $\mathbb{Q}/2\mathbb{Z}$ lies in their 2-torsion subgroups

Note that $(\mathbb{Q}/2\mathbb{Z})_p \simeq (\mathbb{Q}/\mathbb{Z})_p$ if $p \neq 2$, whereas $(\mathbb{Q}/2\mathbb{Z})_2$ is an extension of $\mathbb{Z}/2$ by $(\mathbb{Q}/\mathbb{Z})_2$:

$$0 \to (\mathbb{Q}/\mathbb{Z})_2 \to (\mathbb{Q}/2\mathbb{Z})_2 \to \mathbb{Z}/2 \to 0$$

$$\mathbb{Q}/\mathbb{Z} \simeq \prod_p \mathbb{Z}[1/p]/\mathbb{Z} \text{ and } \mathbb{Q}/2\mathbb{Z} \simeq \prod_p \mathbb{Z}[1/p]/2\mathbb{Z}$$

quadratic form $q\colon \Lambda^\#/\Lambda \to \mathbb{Q}/2\mathbb{Z}$. The underlying bilinear form induces a finite bilinear form

If (Λ, q) is even (hence classically integral with even diagonal) then for each $x, y \in \Lambda^\#$, a counterclockwise twist of the particle $[x] \in \Lambda^\#/\Lambda$ multiplies the wavefunction by the phase

$$\theta_{[x]} = e^{\pi i q(x)} = e^{\pi i q([x])},$$

where $\bar{q}\colon \Lambda^\#/\Lambda \to \mathbb{Q}/2\mathbb{Z}$ is the induced quadratic form on the discriminant group.

Braiding the pair through a full counterclockwise twist gives a phase

$$\theta_{[x],[y]} = e^{\pi i(q(x+y)-q(x)-q(y))} = e^{\pi i B_q(x,y)} = e^{2\pi i q(x,y)} = e^{2\pi i \mathbf{q}([x],[y])},$$

where $\mathbf{q}\colon \Lambda^\#/\Lambda \times \Lambda^\#/\Lambda \to \mathbb{Q}/\mathbb{Z}$ is defined via

$$\mathbf{q}([x],[y]) = q(x,y) \bmod \mathbb{Z} = \frac{\mathbf{q}([x]+[y]) - \mathbf{q}([x]) - \mathbf{q}([y])}{2} \bmod \mathbb{Z}.$$

A subgroup $\mathcal{L} \subset \Lambda^\#/\Lambda$ is **isotropic** if $\mathbf{q}|_{\mathcal{L}\times\mathcal{L}} = 0$. A maximal isotropic subgroup is called **Lagrangian**.

We have $(\mathbb{Z}^n, K)^\# \simeq (\mathbb{Z}^n, K^{-1})$ and $\Lambda^* \simeq (\mathbb{Z}^n, \frac{1}{2}K_{ij}^{-1})$. Note that $[\Lambda^* : \Lambda^\#] = 2^{\operatorname{rank}(\Lambda)}$ and in fact we have extensions

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda^\# & \longrightarrow & \Lambda^* & \longrightarrow & (\mathbb{Z}/2)^n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \vdots & & \\ 0 & \longrightarrow & \Lambda^\#/\Lambda & \longrightarrow & \Lambda^*/\Lambda & \longrightarrow & (\mathbb{Z}/2)^n & \longrightarrow & 0. \end{array}$$

The following lattices can be embedded into the hyperbolic plane $(\mathbb{R}^2, x_1x_2)$:

- $H = (\mathbb{Z}^2, x_1x_2)$ is integral but not classically integral
- $(\mathbb{Z}^2, 2x_1x_2) = \left(\mathbb{Z}^2, x^T \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} x\right) = [2]H$ is classically integral and even
- $(\mathbb{Z}^2, x_1^2 - x_2^2) = \left(\mathbb{Z}^2, x^T \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} x\right)$ is classically integral and odd

III.8 Genera of quadratic $\mathbb{Z}$-lattices

Let $\mathbb{Z}_{(m)} \subset \mathbb{Q}$ be the localization of $\mathbb{Z}$ away from the ideal $(m) = m\mathbb{Z}$. It is the ring of all fractions whose denominator is relatively prime to m. If p is prime, then $\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p$ is a local ring with unique maximal ideal $p\mathbb{Z}_{(p)}$. Two quadratic $\mathbb{Z}$-lattices L and L' are in the same **genus** if they satisfy any of the following equivalent conditions:

- $L_{\mathbb{R}} \simeq L'_{\mathbb{R}}$ and $L_{\mathbb{Z}_p} \simeq L'_{\mathbb{Z}_p}$ for every prime p
- $L_{\mathbb{Z}_{(p)}} \simeq L'_{\mathbb{Z}_{(p)}}$ for every prime p
- $L_{\mathbb{Z}_{(m)}} \simeq L'_{\mathbb{Z}_{(m)}}$ for every $m \in \mathbb{Z}$
- $L_{\mathbb{R}} \simeq L'_{\mathbb{R}}$ and $(L^*/L, q \bmod R) \simeq (L'^*/L', \bar{q}')$

If L and L' are in the same genus, then they are rationally equivalent (i.e. $L_{\mathbb{Q}} \simeq L'_{\mathbb{Q}}$) by the Hasse-Minkowski theorem.

Two quadratic lattices L and L' in the same genus are in the same **spinor genus** if there is an isometry $W\colon L'_{\mathbb{Q}} \to L_{\mathbb{Q}}$ such that there are $g_p \in \mathrm{Spin}(L_{\mathbb{Q}_p})$ with $W(L'_{\mathbb{Z}_p}) = g_p(L_{\mathbb{Z}_p})$ for every p.

Here is the folk theorem stated in Conway and Sloane and proved (among other things) in Brian's Theorem A.5:

Theorem. *Two classically integral lattices (L, q) and (L', q') are in the same genus iff $L \oplus U \simeq L' \oplus U$ (σ_x-equivalence in Cano et al).*

Proof. Using discriminant forms, it is (comparatively) easy to prove that L and L' are in the same genus if $L \oplus U \simeq L' \oplus U$, so we focus on the other direction.

If L and L' are in the same genus, then $L_{\mathbb{R}} \simeq L'_{\mathbb{R}}$ and $L_{\mathbb{Z}_p} \simeq L_{\mathbb{Z}_p}$ for every p. Then $L_{\mathbb{R}} \oplus U_{\mathbb{R}} \simeq L'_{\mathbb{R}} \oplus U_{\mathbb{R}}$ and $L_{\mathbb{Z}_p} \oplus U_{\mathbb{Z}_p} \simeq L'_{\mathbb{Z}_p} \oplus U_{\mathbb{Z}_p}$ for every p, hence $L \oplus U$ and $L' \oplus U$ are also in the same genus. We will show that they are in the same spinor genus. For this we note the Corollary to Lemma 11.3.6 in [4]:

> *Suppose that $\mathbb{Z}_p^\times(\mathbb{Q}_p^\times)^2 \subset \nu(\mathrm{SO}(\Lambda_{\mathbb{Z}_p}))$ for every p. Then the genus of Λ contains exactly one spinor genus.*

Because $\mathrm{SO}(L_{\mathbb{Z}_p}) \times \mathrm{SO}(U_{\mathbb{Z}_p}) \subset \mathrm{SO}(L_{\mathbb{Z}_p} \oplus U_{\mathbb{Z}_p})$, the spinor norms satisfy

$$\nu(\mathrm{SO}(L_{\mathbb{Z}_p})) \cup \nu(\mathrm{SO}(U_{\mathbb{Z}_p})) \subset \nu(\mathrm{SO}(L_{\mathbb{Z}_p} \oplus U_{\mathbb{Z}_p})).$$

Therefore, if we can show that $\mathbb{Z}_p^\times \bmod (\mathbb{Q}_p^\times)^2 \subset \nu(\mathrm{SO}(U_{\mathbb{Z}_p}))$ for every p, we can apply the corollary with $\Lambda = L \oplus H$ to complete the proof. But this follows by Lemma 11.3.7 ($p \neq 2$) and Lemma 11.3.8 ($p = 2$) in [4].

Therefore, $L \oplus U$ and $L' \oplus U$ are in the same spinor genus. Since $L \oplus U$ is indefinite of rank at least 3, Eichler's theorem implies that $L \oplus U \simeq L' \oplus U$.

□

Note that the proof of the "easy" direction $L \oplus U \simeq L' \oplus U \Rightarrow \mathrm{Genus}(L) = \mathrm{Genus}(L')$ has a physical interpretation even if we replace U with any unimodular lattice whatsoever.

Chapter IV
Algebras over fields

IV.1 Characteristic polynomial, norm and trace

Each algebra over an integral domain R contains a copy $R \cdot 1$ of R through its action on the identity 1, i.e the natural map from R is injective because there are no zero divisors. In particular, such algebras can (and will) be studied as subalgebras of algebras over their fraction fields $K = \mathrm{Frac}(R) = R_{(0)}$. Here we recall the structure of such algebras.

Let A be an algebra over a field K of dimension $m = \dim_K(A)$. Left multiplication by $a \in A$ is a linear map $\ell_a \in \mathrm{End}_K(A)$ whose **characteristic polynomial**

$$\det(xI - \ell_a) = x^m - \mathrm{Tr}_{A/K}(a)x^{m-1} + \cdots + (-1)^m \,\mathrm{N}_{A/K}(a) \in K[x]$$

defines the **norm** $\mathrm{N}_{A/K}(a) = \det(\ell_a)$ and **trace** $\mathrm{Tr}_{A/K}(a) = \mathrm{Tr}(\ell_a)$ from A to K. The algebra A can be viewed as a $K[x]$-module on which $g(x)$ acts via left-multiplication by $g(a)$, i.e. via $g(\ell_a) \in \mathrm{End}_K(A)$. As $K[x]$-modules, $A \simeq \bigoplus_i K[x]/(f_i(x))$, where $\prod_i f_i(x)$ is the factorization of the characteristic polynomial into irreducible monic factors. The gcd of the f_i is the **minimal polynomial** of a over K which, unlike the characteristic polynomial, is independent of the ambient algebra A (i.e. unchanged under embeddings of A or $K(a)$ into larger K-algebras). The **degree** of a over K is the degree of its minimal polynomial and the **degree** $[A : K]$ of A over K is the maximum degree of its elements.

IV.2 Semisimple algebras

By the Artin-Wedderburn Theorem I.5.2, each semisimple K-algebra is isomorphic to a finite product

$$A_1 \times \cdots \times A_r$$

of simple algebras A_i/K. The center of each simple component A_i is a finite extension F_i of K. For each $a \in A_i$, the characteristic polynomial of $\ell_a \in \mathrm{End}_{F_i}(A_i)$ has the form

$$\det(x - \ell_a) = \Big(x^{n_i} - \mathrm{Trd}(a)x^{n_i-1} + \cdots + (-1)^{n_i} \,\mathrm{Nrd}(a)\Big)^{n_i} \in F_i[x],$$

where the **reduced characteristic polynomial**

$$x^{n_i} - \mathrm{Trd}(a)x^{n_i-1} + \cdots + (-1)^{n_i} \,\mathrm{Nrd}(a) \in F_i[x]$$

defines the **reduced trace** $\mathrm{Trd}\colon A_i \to F_i$ and **reduced norm** $\mathrm{Nrd}\colon A_i \to F_i$, for which

$$\mathrm{Tr}_{A_i/F_i}(a) = n_i \,\mathrm{Trd}_{A_i/F_i}(a), \quad \mathrm{N}_{A_i/F_i}(a) = \mathrm{Nrd}^{n_i}_{A_i/F_i}\,.$$

These maps extend to the simple algebras A_i/K by composing with the relative trace and norm

$$\mathrm{Trd}_{A_i/K} = \mathrm{Tr}_{F_i/K} \circ \mathrm{Trd}_{A/F_i}, \quad \mathrm{Nrd}_{A_i/K} = \mathrm{N}_{F_i/K} \circ \mathrm{Nrd}_{A/F_i},$$

and finally to the semisimple algebra A/K via

$$\mathrm{Trd}_{A/K}(a_1, \ldots, a_r) = \sum_i \mathrm{Trd}_{A_i/K}(a_i) = \sum_i \mathrm{Tr}_{F_i/K} \circ \mathrm{Trd}_{A_i/F_i}(a_i)$$

and

$$\mathrm{Nrd}_{A/K}(a_1, \ldots, a_r) = \prod_i \mathrm{Nrd}_{A_i/K}(a_i) = \prod_i \mathrm{N}_{F_i/K} \circ \mathrm{Nrd}_{A_i/F_i}(a_i).$$

Given an involution σ on A and a $u \in A^\times$ fixed by σ, the corresponding **twisted trace form** is the sesquilinear form

$$T_{(\sigma,u)}(x, y) = \mathrm{Trd}_{A/K}(\sigma(x)uy).$$

IV.2.1 Separability

Let K be a field. A polynomial in $K[x]$ is **separable** if it has distinct roots in some algebraic extension of K. It is well known that $f(x)$ is separable iff $f(x)$ and $f'(x)$ are relatively prime, i.e. have no common roots. If K has characteristic 0 then every polynomial in $K[x]$ is separable so inseparability can only occur in prime characteristic.

Each irreducible inseparable polynomial in $K[x]$ has a unique representation $f(x^{p^m})$ for a irreducible separable polynomial $f \in K[x]$ an integer $m \geq 2$. Therefore the degree of any irreducible inseparable polynomial is a multiple of the characteristic. Because degrees add under products, the degree of any inseparable polynomial is a multiple of the characteristic. For example, $x^p - 1 \in \mathbb{F}_p[x]$ is inseparable because the freshman's dream $x^p - 1 = (x-1)^p$ holds in $\mathbb{F}_p[x]$.

An element of an algebraic field extension F/K is **separable** if its minimal polynomial over K is separable. An algebraic field extension F/K is **separable** if every element is separable.

A field extension is **separable** [20] if the minimal polynomial of every finitely generated subextension is separable.

A semisimple algebra A/K is separable iff it satisfies any of the following equivalent conditions:

- The trace pairing $(a, b) \mapsto \mathrm{Trd}_{A/K}(ab)$ from $A \times A \to K$ is nondegenerate.
- If σ is an involution on A fixing a unit $u \in A^\times$, then the twisted trace form $T_{(\sigma,u)}$ is nondegenerate.
- $A \otimes_K F$ is semisimple for every field extension F/K.

Separable field extensions may be further characterized as follows: A **derivation** on a ring R is an R-bimodule-valued function $\delta\colon R \to M$ that is a homomorphism of abelian groups $\delta(x+y) = \delta(x) + \delta(y)$ and satisfies Leibnitz's formula $\delta(xy) = \delta(x)y + x\delta(y)$. The following conditions on a finite-degree field extension F/K are also equivalent:

- F/K is separable.
- $\mathrm{Tr}_{F/K} \neq 0$.
- $\mathrm{Tr}_{F/K}(F) = K$.
- Every derivation $K \to K$ has a unique extension to a derivation $L \to L$.

Finally we have the following equivalent conditions on a semisimple algebra A/K:

- A/K is separable.
- A/K is a finite product of central simple algebras over finite separable extensions of K.
- There exists a finite separable extension F/K such that $A \otimes_K F$ is a direct sum of matrix algebras over F.

IV.2.2 Perfect fields

A field K is called **perfect** if every finite extension F/K is separable. Equivalently, K is perfect if every algebraic extension is separable, or if the separable closure is algebraically closed. A field K is imperfect iff it has characteristic p and its Frobenius automorphism has a kernel. If F is perfect of characteristic p, then every nonzero element is a pth power.

IV.2.3 Brauer group

By the Artin-Wedderburn Theorem I.5.2, A is simple iff it is isomorphic to $D^{\kappa\times\kappa}$ for some central division algebra D/K of degree m, satisfying $n = \kappa m$. Two central simple K-algebras A_1 and A_2 are similar (written $A_1 \sim A_2$) if there is an isomorphism $A_1^{m\times m} \to A_2^{n\times n}$ of K-algebras for some integers m and n. Equivalently, $A_1 \sim A_2$ if their underlying division algebras are isomorphic over K. The corresponding equivalence classes make up the **Brauer group** $\mathrm{Br}(K)$ with multiplication rule $[A]\cdot[B] = [A \otimes_K B]$ and inverse $[A]^{-1} = [A^{op}]$, where A^{op} is the **opposite algebra** with multiplication $X \cdot Y = YX$. In particular, if $A_1 \simeq D_1^{n\times n}$ and $A_2 \simeq D_2^{m\times m}$ for central division algebras D_1 and D_2 over K, then we have $A_1 \sim A_2$ iff $[A_1] = [A_2]$ iff $D_1 \simeq D_1$. In particular, $[A]$ is the trivial element of $\mathrm{Br}(K)$ precisely when there exists a K-isomorphism $K^{n\times n} \to A$, in which case A is said to **split**.

For example, the Brauer groups of $\mathbb{R}$ and $\mathbb{C}$ exhaust the possible isomorphism classes of real division algebras, subdivided into those $\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$ that are central over $\mathbb{R}$ and those $\mathrm{Br}(\mathbb{C}) = \{[\mathbb{C}]\}$ that are central over $\mathbb{C}$.

If $[A] = [D]$, the **capacity** is the κ for which $A \simeq D^{\kappa\times\kappa}$, which satisfies

$$n = [D^{\kappa\times\kappa} : K] = \kappa[D : K].$$

The (Schur) **index** of A is the degree $[D : K]$, for which $\dim_K(D) = [D : K]^2$. The **exponent**, or *period*, of A is the order of $[A] = [D] \in \mathrm{Br}(K)$. The exponent and period are equal if the center of A is a separable field extension, i.e. if A is a separable algebra. In general, the period and the index have the same prime factors while the exponent divides the index, so they always coincide if the index is squarefree. If $A \simeq D^{\kappa\times\kappa}$, then [1] calls κ the **capacity** of A, in which case we have $n = \kappa m$ where m is the index.

IV.2.4 Relative Brauer group

If A/K is a central simple K-algebra and F/K is an extension field, then $A_F := A \otimes_K F$ is a new central simple F-algebra obtained by extending scalars from K to F. The corresponding map $[A] \mapsto [A_F]$ from $\mathrm{Br}(K)$ to $\mathrm{Br}(F)$ is a homomorphism (in fact, we have a functor $\mathrm{Br}\colon \mathsf{Fields} \to \mathsf{Ab}$)) whose image is trivial iff A_F is a matrix algebra over F, in which case we say that F **splits** A. In such a case, we obtain a matrix representation of A over F.

On the other hand, $\mathbb{R} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C}$ and $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C}^{2\times 2}$.

The **relative Brauer group** $\mathrm{Br}(K/k)$ contains the Brauer classes of central simple algebras A/k split by K and sits in the exact sequence

$$1 \to \mathrm{Br}(K/k) \to \mathrm{Br}(k) \to \mathrm{Br}(K) \to 1$$

where the last map takes $[A] \in \mathrm{Br}(k)$ to $[A_K] \in \mathrm{Br}(K)$. We will see later that there are cohomological interpretations

$$\mathrm{Br}(K/k) \simeq H^1(\mathrm{Gal}(K/k), \mathrm{PGL}_\infty(K)) \simeq H^2(\mathrm{Gal}(K/k), K^\times)$$

and

$$\mathrm{Br}(k) \simeq H^1(\mathrm{Gal}(k_s/k), \mathrm{PGL}_\infty(k_s)) \simeq H^2(\mathrm{Gal}(k_s/k), k_s^\times),$$

where k_s denotes a separable closure of k.

IV.3 Galois cohomology

IV.3.1 $H^1(G, C)$ with possibly nonabelian C

Given a left action of a group G on a potentially nonabelian group C, a **1-cocycle** is a function $c\colon G \to C$ satisfying

$$c_{\sigma_1\sigma_2} = c_{\sigma_1}\sigma_1(c_{\sigma_2}) \tag{IV.1}$$

for every $\sigma_1, \sigma_2 \in G$. Call two 1-cocycles $c, c' \colon G \to C$ **equivalent**, or **cohomologous**, if there is a $\gamma \in C$ such that

$$c'_\sigma = \gamma^{-1} c_\sigma \sigma(\gamma) \tag{IV.2}$$

for every $\sigma \in G$. The corresponding equivalence classes comprise the **first cohomology set** $H^1(G, C)$, which is a pointed set whose distinguished element is the class of the trivial cocycle $c_\sigma = 1$.

When C is abelian, the 1-cocycles form an abelian group under pointwise multiplication (or addition, as they are often written additively in this case) and are sometimes called **crossed homomorphisms**. The 1-coboundaries (now a subgroup) are sometimes called **principal crossed homomorphisms**. Then $H^1(G, C)$ can be constructed as the quotient group {1-cocycles}/{1-coboundaries}, in which case it classifies splittings of

$$1 \to C \to C \rtimes G \to G \to 1$$

where two splittings $s, s' \colon G \to C \rtimes G$ are equivalent if there is an $c \in C$ such that $s'(g) = cs(g)c^{-1}$ for every $g \in G$.

For nonabelian C, the equivalence relation (IV.2) is defined directly, rather than by modding out by 1-coboundaries, as there is no obvious group structure on the set of 1-cocycles when A is nonabelian.

An important application of nonabelian 1-cocycles considers a set X equipped with compatible actions by G and C, satisfying

$$\sigma(c(x)) = (\sigma(c))(\sigma(x)) \tag{IV.3}$$

for every $\sigma \in G$, $c \in C$ and $x \in X$. Then each 1-cocycle $c \colon G \to C$ gives rise to a corresponding **twisted group action**

$$\sigma \cdot_c x = c_\sigma(\sigma(x)) \tag{IV.4}$$

of G on X. The cocycle condition is exactly what is needed for $\cdot_c$ to define a group action:

$$\begin{aligned} \sigma \cdot_c (\tau \cdot_c x)) &= \sigma \cdot_c (c_\tau(x^\tau) = c_\sigma(c_\tau(\tau(x))^\sigma) = c_\sigma(c_\tau^\sigma(x^{\sigma\tau}) = (c_\sigma c_\tau^\sigma)(x^{\sigma\tau}) \\ &= c_{\sigma\tau}(x^{\sigma\tau}) = (\sigma\tau) \cdot_c x. \end{aligned}$$

Write ${}_cX$ for the set X equipped with this action. While cohomologous 1-cocycles generally give rise to distinct twisted actions, Galois descent theory provides a natural setting identifying the corresponding cohomology classes with Brauer equivalence classes of central simple algebras.

IV.3.2 $H^2(G, A)$ with abelian A

Let A be a G-module. A **2-cocycle** (a.k.a. a **factor set**) is a function $a \colon G \times G \to A$ such that

$$a_{\sigma_1, \sigma_2\sigma_3} a_{\sigma_2, \sigma_3} = a_{\sigma_1\sigma_2, \sigma_3} \sigma_3(a_{\sigma_1, \sigma_2}).$$

A 2-cocycle a is a **2-coboundary** if there exists a 1-cocycle $b\colon \mathrm{Gal}(F/K) \to K^\times$ such that

$$a_{\sigma_1,\sigma_2} = \frac{\sigma_2(b_{\sigma_1})b_{\sigma_2}}{b_{\sigma_1\sigma_2}}.$$

The 2-cocycles form an abelian group under pointwise multiplication with respect to which the 2-coboundaries are a subgroup. The quotient group is the second cohomology group $H^2(G, A)$.

Proposition 4.4.1 from [7]. *Let*

$$1 \to A \xrightarrow{i} B \xrightarrow{j} C \to 1 \tag{IV.5}$$

be an exact sequence of groups acted on by some group G, such that A is commutative and contained in the center of B. Then there is an exact sequence of pointed sets

$$1 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \xrightarrow{\delta} H^2(G, A) \to H^2(G, B) \to$$

where the connecting homomorphism δ takes the class of a 1-cocycle $c\colon G \to C$ to the class of the 2-cocycle $a\colon G \times G \to A$ defined by $i(a_{\sigma,\tau}) = b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$, where $b_\sigma = j^{-1}(c_\sigma)$ for an arbitrary lifting $j^{-1}\colon C \to B$. As a function of c, a depends only on the class of c. The class of c is independent of the particular lifting j^{-1} from C to B.

IV.3.3 Twisted forms

A K**-object** (V, Φ) consists of a vector space V/K and a tensor $\Phi \in V^{\otimes n} \otimes (V^*)^{\otimes n'}$. Two K-objects (V, Φ) and (W, Ψ) are **isomorphic** if there exists a K-linear isomorphism $f\colon V \to W$ such that $f^{\otimes n} \otimes (f^{*-1})^{\otimes n'}(\Phi) = \Psi$. For each field extension F/K, let (V_F, Φ) be the corresponding F-object, whose underlying vector space is $V_F = V \otimes_K F$. If (V, Φ) and (W, Ψ) are not isomorphic, they may **become isomorphic** over an extension F/K, meaning that there is an F-isomorphism between the corresponding F-objects (V_F, Φ) and (W_F, Ψ). For reasons explained below, W is called a **twisted form** of V when the two become isomorphic over some extension.

Let (V, Φ) and (W, Ψ) be K-objects becoming isomorphic over a finite Galois extension F/K. Then there is a natural action of $\mathrm{Gal}(F/K)$ on (V_F, Φ) and on (W_F, Ψ). Correspondingly, $\mathrm{Gal}(F/K)$ also acts on the space of F-isomorphisms from V_F to W_F and on the automorphism group $\mathrm{Aut}(V_F, \Phi)$ via $\sigma(f) = \sigma f \sigma^{-1}$. Then $\mathrm{Gal}(F/K)$ and $\mathrm{Aut}(V_F, \Phi)$ act compatibly on (V_F, Φ) in the sense of (IV.3), where we take

$$G = \mathrm{Gal}(F/K),\ A = \mathrm{Aut}(V_F, \Phi) \text{ and } X = (V_F, \Phi).$$

A given F-isomorphism $f\colon (V_F, \Phi) \to (W_F, \Psi)$ will not generally be equivariant for the natural actions of $\mathrm{Gal}(F/K)$ on (V_F, Φ) and (W_F, Φ). In fact, we will see that unless W and V are already isomorphic over K, no such F-isomorphism can exist. However, f *is* equivariant if we twist the Galois action on V_F by the 1-cocycle $c\colon \mathrm{Gal}(F/K) \to \mathrm{Aut}(V_F, \Phi)$ given by

$$c_\sigma := f^{-1}\sigma(f) = f^{-1}\sigma f \sigma^{-1} \tag{IV.6}$$

(see Section 2.3 of [7] for the calculation showing that c_σ is indeed a 1-cocycle), so that the following diagram commutes

$$\begin{array}{ccc} {}_cV_F & \xrightarrow{f} & W_F \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} \\ {}_cV_F & \xrightarrow{f} & W_F \end{array}$$

(recall that σ acts on V_F as $c_\sigma\sigma$). Taking $\mathrm{Gal}(F/K)$ invariants shows that f restricts to an isomorphism $({}_cV_F)^{\mathrm{Gal}(F/K)} \to W$, realizing (W,Ψ) as a **twisted form** of (V,Φ).

If $f'\colon (V_F,\Phi) \to (W_F,\Psi)$ is another F-isomorphism, then the corresponding 1-cocycle c'_σ is cohomologous to c_σ because (IV.2) holds with $b = f^{-1}f'$, i.e.

$$b^{-1}c_\sigma\sigma(b) = f'^{-1}f \quad f^{-1}\sigma f\sigma^{-1} \quad \sigma f^{-1}f'\sigma^{-1} = f'^{-1}\sigma f'\sigma^{-1} = c'_\sigma.$$

On the other hand, the invariant subalgebras of $F^{n\times n}$ for the twisted Galois actions associated to cohomologous 1-cocycles are K-isomorphic (see e.g. Theorem 2.3.3 of [7]), giving a bijection between $H^1(\mathrm{Gal}(F/K), \mathrm{Aut}(V_F,\Phi))$ and the pointed set of F/K-twisted forms of (V,Φ).

IV.3.4 Central simple algebras are twisted matrix algebras

Each central simple algebra A/K determines a K-object (A, mult_A), where $\mathrm{mult}_A \in A^* \otimes A^* \otimes A$ is the tensor corresponding to the algebra multiplication $A \times A \to A$. The Skolem-Noether theorem implies that every automorphism of A is inner, so

$$\mathrm{Aut}(A) = \{x \mapsto axa^{-1} : a \in A^\times\} = A^\times/K^\times.$$

When $A = K^{n\times n}$,

$$\mathrm{Aut}(K^{n\times n}) = \mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/K^\times,$$

so there is an exact sequence

$$1 \to K^\times \to \mathrm{GL}_n(K) \to \mathrm{PGL}_n(K) \to 1.$$

Now suppose that F/K is a finite Galois extension that splits A. Then the above implies that the F-isomorphism $f\colon {}_aF^{n\times n} \to A_F$ is equivariant for the $\mathrm{Gal}(F/K)$ action on $F^{n\times n}$ obtained by twisting the canonical action by the $\mathrm{PGL}_n(F)$-valued 1-cocycle $a_\sigma = f^{-1}\sigma f\sigma^{-1}$.

The F-isomorphism f restricts to a K-isomorphism

$$\tilde{f}\colon ({}_aF^{n\times n})^{\mathrm{Gal}(F/K)} \to A,$$

realizing the central simple algebra A/K as a twisted form of $K^{n\times n}$.

Theorem 2.4.3 of [7] shows that there is a basepoint-preserving bijection between the first cohomology set $H^1(\mathrm{Gal}(F/K), \mathrm{PGL}_n(F))$ and the pointed set $\mathrm{CSA}_n(F/K)$ of K-isomorphism classes of central simple K-algebras of degree n that are split by F. This is

because the elements of $\mathrm{CSA}_n(F/K)$ are precisely the F/K-twisted forms of the matrix algebra $K^{n\times n}$.

Corollary 2.4.10 of [7] gives a similar bijection between $H^1(\mathrm{Gal}(F/K),\mathrm{PGL}_\infty(F))$ and the relative Brauer group $\mathrm{Br}(F/K)$, whose elements are equivalence classes of central simple simple K-algebras (of any degree) that are split by F. Then $H^1(\mathrm{Gal}(F/K),\mathrm{PGL}_\infty(F))$ inherits an abelian group structure through this bijection, even though the coefficient group is not abelian. The union

$$H^1(K,\mathrm{PGL}_\infty) := \bigcup_{K^\mathrm{s}\supset F\supset K} H^1(\mathrm{Gal}(F/K),\mathrm{PGL}_\infty(F))$$

over all extensions contained in a separable closure K^s is in bijection with the Brauer group $\mathrm{Br}(K)$.

It is possible to work with abelian coefficients by going one level higher in cohomology.

Applying Proposition 4.4.1 of [7] to the exact sequence

$$1 \to F^\times \to \mathrm{GL}_n(F) \to \mathrm{PGL}_n(F) \to 1$$

gives a long exact sequence

$$\to H^1(G,\mathrm{GL}_n(F)) \to H^1(G,\mathrm{PGL}_n(F)) \xrightarrow{\delta_n} H^2(G,F^\times) \to H^2(G,\mathrm{GL}_n(F)) \to .$$

Given a 1-cocycle $\sigma\mapsto c_\sigma\in\mathrm{PGL}_n(F)$, let b_σ be an arbitrary lifting to $\mathrm{GL}_n(F)$ and let $a_{\sigma,\tau}$ be the $F^\times$-valued 2-cocycle defined by $a_{\sigma,\tau}I = b_\sigma\sigma(b_\tau)b_{\sigma\tau}^{-1}$. Then the connecting homomorphism δ_n maps the class of c in $H^1(\mathrm{Gal}(F/K),\mathrm{PGL}_n(F))$ to the class of a in $H^2(\mathrm{Gal}(F/K),F^\times)$.

What does this say about our 1-cocycle $g_\sigma = \sigma^{-1}f\sigma f^{-1}$ coming from an isomorphism $f\colon F^{n\times n}\to A\otimes_K F$? Let $\iota\colon F\to A$ be an embedding of a degree n Galois extension F/K of a number field K into a central simple algebra A/K with $\dim_K(A)=n^2$. Then A is an F-vector space of dimension n with respect to the action $\alpha\cdot a = a\iota(\alpha)$. There is a corresponding left action of A on this vector space, identifying A with a K-subalgebra of $\mathrm{End}_F(\mathrm{End}_F(A))\simeq F^{n\times n}$.

Each δ_n is an injective map of pointed sets. These maps satisfy $\delta_{nm}|_{H^1(\mathrm{Gal}(F/K),\mathrm{PGL}_n(F))} = \delta_n$ for all $n,m\in\mathbb{N}$, where we identify $F^{n\times n}$ with its image $F^{nm\times nm}$ under the injective F-algebra homomorphism $X\mapsto X\otimes_F I_m$. The corresponding direct limit

$$\delta\colon H^1(\mathrm{Gal}(F/K),\mathrm{PGL}_\infty(F))\to H^2(\mathrm{Gal}(F/K),F^\times)$$

is an isomorphism of pointed sets (see Theorem 4.4.5 of [7]).

Each 2-cocycle $a\colon G\times G\to F^\times$ on $G=\mathrm{Gal}(F/K)$ determines a central simple K-algebra

$$F(G,a) = \left\{\sum_\sigma x_\sigma u_\sigma : u_\sigma x u_\sigma^{-1} = \sigma(x), u_\sigma u_\tau = a_{\sigma,\tau}u_{\sigma\tau}\right\}$$

called a crossed product, that is split by F and can be viewed as an a-twisted version of the group algebra $F(G)$. The K-isomorphism class of $F(G,a)$ only depends on the

cohomology class $[a] \in H^2(G, F^\times)$ of a and if $b\colon G^2 \to F^\times$ is another 2-cocycle, the Brauer classes satisfy $[F(G,a) \otimes_K F(G,b)] = [F(G,ab)]$. If $G = \langle\sigma\rangle$ is cyclic of order n, then there exists an $\alpha \in F^\times$ such that $[a]$ is represented by the 2-cocycle

$$a_{\sigma,\tau} = \begin{cases} \alpha & \text{if } \sigma\tau = 1 \\ 1 & \text{otherwise} \end{cases}$$

and the corresponding crossed product is called a cyclic algebra

$$F(G,a) = F(G,\alpha) = \left\{ \sum_\sigma x_\sigma u_\sigma : u_\sigma x u_\sigma^{-1} = \sigma(x), u^n = \alpha \right\}.$$

Brauer-Hasse-Noether and Albert famously proved that every central simple algebra is cyclic (see e.g. [8]).

IV.4 Quaternion algebras

The quaternion algebras over K correspond exactly to the 2-torsion in the Brauer group $\mathrm{Br}(K)$. Here we have

$$1 \to \mathrm{Br}(K)_2 \to \bigoplus_v \mathrm{Br}(K_v)_2 \xrightarrow{\sum \mathrm{inv}_v} \tfrac{1}{2}\mathbb{Z}/\mathbb{Z} \to 0,$$

where, for a quaternion algebra A/K, we have $\mathrm{inv}_v([A_v]) = 0$ or $\frac{1}{2}$ according to whether or not A_v/K_v splits. In particular, this implies that a quaternion algebra over A is ramified at an even number of primes. For a fixed Galois extension L/K, we would like to characterize the pointed set

$$\mathrm{CSA}_2(L/K) = \{\text{isomorphism classes of quaternion } K\text{-algebras split by } L\}.$$

Galois descent gives a bijection $\mathrm{CSA}_2(L/K) \simeq H^1(\mathrm{Gal}(L/K), \mathrm{PGL}_2(L))$ of pointed sets. The cohomology of the extension

$$1 \to L^\times \to \mathrm{GL}_2(L) \to \mathrm{PGL}_2(L) \to 1$$

is given by

cohomology sequence here with connecting homomorphism

so that in turn, $H^1(\mathrm{Gal}(L/K), \mathrm{PGL}_2(L))$ can be viewed as a subgroup of

$$H^2(\mathrm{Gal}(L/K), L^\times) \simeq \mathrm{Br}(L/K) := \{[A] \in \mathrm{Br}(K) : A_L \text{ splits}\}.$$

Restricting to the 2-torsion subgroups gives

$$1 \to \mathrm{Br}(L/K)_2 \to \mathrm{Br}(K)_2 \to \mathrm{Br}(L)_2 \to 1.$$

For example, the field $L = \mathbb{Q}(\sqrt{m})$ splits $A = \left(\frac{a,b}{\mathbb{Q}}\right)$ iff, for every ramified place v of $\mathbb{Q}$, $\mathbb{Q}_v(\sqrt{m})$ is a field (i.e. $m \notin \mathbb{Q}_v^2$). For $\left(\frac{-1,-1}{\mathbb{Q}}\right)$, this amounts to requiring that $m < 0$ and $-m \neq 4^a(7+8b)$.

IV.5 K-algebras with involution

Let $h\colon V \times V \to F$ be a nonsingular hermitian form on V/F, where F/F_+ is a quadratic extension. The adjoint involution $\sigma_h(a) = h^{-1}a^*h$ is F/F_+-antilinear, and there is a 1-1 correspondence between such involutions and equivalence classes of hermitian forms modulo multiplication by scalars in $F_+^\times$.

Let F/K be a splitting field for A, so that $A \otimes_K F \simeq \mathrm{End}_F(V)$ for some vector space V/F. Let σ_F be the extension of σ to $\mathrm{End}(V)$. If σ is of the first kind, then σ_F is the

adjoint involution for a bilinear form b_σ that is uniquely determined up to scalars in $F^\times$; σ is **symplectic** if b_σ is alternating and **orthogonal** if b_σ is symmetric. If σ is of the second kind, then σ_F is adjoint to a hermitian form h_σ. Involutions of the second kind are also called **unitary**.

By an **involuted field** $(K/k, j)$, we mean an étale algebra K over a field k, equipped with an involution $j\colon K \to K$ whose set of fixed points is k. Hence either j is trivial and $K = k$, or else j is nontrivial and there are two possibilties: either K/k is a quadratic separable field extension with nontrivial Galois automorphism j, or $K = k \times k$ is a "doubled field" with j equal to the swap $s(x, y) = (y, x)$. By a central simple algebra over $k \times k$, we will mean a direct product of central simple k-algebras.

Given an involuted field $(K/k, j)$, Wall [21] first considers involuted algebras (A, J) consisting of a central simple K-algebra A with involution J restricting to j on the center. He defines an equivalence relation such that the class $((A, J))$ of (A, J) contains the involuted algebras of the form $(A \otimes K^{n\times n}, J \otimes J_n)$, where $J_n\colon K^{n\times n} \to K^{n\times n}$ is the adjoint involution for some nondegenerate j-hermitian form on K^n. There is a group structure on the equivalence classes, where $((A_1, J_1)) \cdot ((A_1, J_2)) = ((A_1 \otimes_K A_2, J_1 \otimes J_2))$ and where $((A, J))^{-1} = ((A^{\mathrm{op}}, J^{\mathrm{op}}))$, with J^{op} defined as $J^{\mathrm{op}}(a^{\mathrm{op}}) = J(a)^{\mathrm{op}}$. The resulting group $\mathrm{Br}(K/k, j)$ is also a functor from involuted fields to abelian groups.

IV.5.1 Involutions on quaternion algebras

The involutions on a quaternion algebra A are completely classified (see e.g. Proposition 2.21 of [2]). Every involution of the first kind on A has the form $\sigma_u(a) = u\bar{a}u^{-1}$ for some nonzero quaternion u satisfying $\bar{u} = \pm u$, where $a \mapsto \bar{a} = \mathrm{Trd}\, a - a$ is the canonical involution. There are two possibilities: if $\bar{u} = u$, then u is proportional to the identity, giving the canonical involution as the unique symplectic involution. The orthogonal involutions are obtained from pure quaternions $u \in A_0^\times := A_0 \cap A^\times$ (i.e. $\bar{u} = -u$), which are uniquely determined up to multiplication by scalars in $F^\times$.

A central simple algebra A/K equipped with a unitary involution τ may be viewed as a central simple involuted algebra $(A, \tau)/(K/K_+, c)$. Restricting scalars to K_+ turns A into a semisimple K_+-algebra containing a unique quaternion K_+-subalgebra B (the **discriminant algebra** – see ğ10 of [2]) such that $(A, \tau) \simeq (B \otimes_{K_+} K, \bar{\cdot} \otimes c)$.

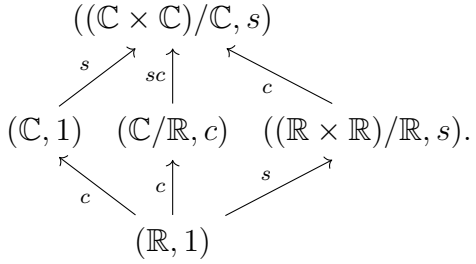
Given a quaternion algebra B/K_+ and a quadratic extension $(K/K_+, c)$ that splits B, let $\phi\colon K^{2\times 2} \to B \otimes_{K_+} K$ be any splitting and define $u := \phi^{-1}\tau\phi\tau = \phi^{-1}\tau(\phi)$. Then I claim that $(K^{2\times 2}, \sigma) \simeq (B \otimes_{K_+} K, \bar{\cdot} \otimes \tau)$, where $\sigma(a) = \iota \cdot_u a = uc(a)u^{-1}$ is complex conjugation in a different basis. Note that even here there is nothing forcing σ to be hermitian conjugation, although in cases where it is, the unit group would be the ordinary unitary group.

IV.5.2 Algebras over real involuted fields

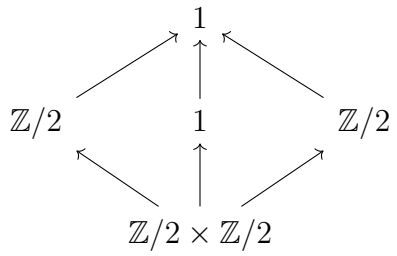
The Galois closure of $\mathbb{R}$ is $\mathbb{C}$ and we have

$$\begin{array}{ccc} \mathrm{Br}(\mathbb{C}) & \longrightarrow & \mathrm{BW}(\mathbb{C}) \\ \uparrow & & \uparrow \\ \mathrm{Br}(\mathbb{R}) & \longrightarrow & \mathrm{BW}(\mathbb{R}) \end{array} \quad = \quad \begin{array}{ccc} 1 & \longrightarrow & \mathbb{Z}/2 \\ \uparrow & & \uparrow \\ \mathbb{Z}/2 & \longrightarrow & \mathbb{Z}/8 \end{array}$$

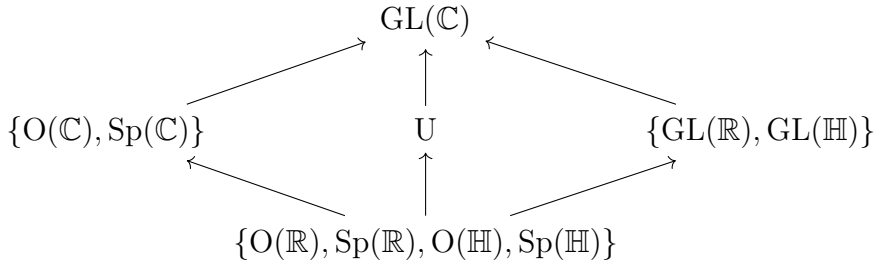
The Galois closure of $(\mathbb{R}, 1)$ is $(\mathbb{C} \times \mathbb{C}, s)$ and its Galois group is $\langle s, c\rangle = (\mathbb{Z}/2)^2$, where c is coordinatewise complex conjugation. The three intermediate involuted fields are as follows, with each arrow labeled by the nontrivial automorphism fixing the included field:



The modified Brauer groups are

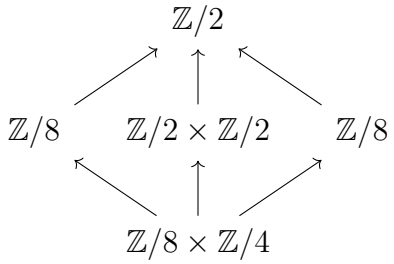


and we have $\mathrm{Br}(\mathbb{R}, 1) \simeq \mathrm{Br}(\mathbb{C}, 1) \times \mathrm{Br}((\mathbb{R} \times \mathbb{R})/\mathbb{R}, s)$. The elements of $\mathrm{Br}(K/k, j)$ correspond to classes of simple involuted algebras (A, J) determining a group $G = \{a \in A : aJ(a) = 1\}$ according to the following possibilities:



We also obtain the special versions $G_1 = \{a \in G : \mathrm{Nrd}(a) = 1\}$ though I'm unclear what changes for the symplectic groups $\mathrm{Sp}(\mathbb{C})$ and $\mathrm{Sp}(\mathbb{H})$. The graded Brauer groups

are


$\mathbb{Z}/2$
$\mathbb{Z}/8$
$\mathbb{Z}/2 \times \mathbb{Z}/2$
$\mathbb{Z}/8$
$\mathbb{Z}/8 \times \mathbb{Z}/4$

Chapter V
Superalgebras

V.1 Superalgebras

A **superalgebra** A over a field K is a K-algebra equipped with a $\mathbb{Z}/2$-grading $A = A_0 + A_1$ into subspaces $A_i \subset A$ with $A_i A_j \subset A_{i+j}$. An $a \in A$ is **homogeneous** if $a \in A_i$ for some i that we call the **degree** $\delta(a)$ of a. A subspace $S \subset A$ is **homogeneous** if it generated by homogeneous elements, in which case $S = S_0 + S_1$ with $S_i = S \cap A_i$.

The center $Z(A)$ of a superalgebra A/K is a superalgebra. Call a superalgebra A/K **central** if $Z(A)_0 \simeq K$ and **simple** if A contains no nontrivial homogeneous ideals. Because a simple superalgebra can have inhomogeneous ideals, it follows that a superalgebra is simple if it is simple as an algebra.

The **supercenter** $\widehat{Z}(A)$ of a superalgebra A/K is the subsuperalgebra generated by homogeneous $z \in A$ such that $za = (-1)^{\delta(z)\delta(a)} az$ for every homogeneous $a \in A$. In other words, $\widehat{Z}(A) = \widehat{Z}(A)_0 + \widehat{Z}(A)_1$ with $\widehat{Z}(A)_0 = Z(A)_0$ but $\widehat{Z}(A)_1$ containing those elements in A_1 commuting with A_0 while *anticommuting* with A_1.

The **tensor product** of two superalgebras A and B is the superalgebra $A \widehat{\otimes} B$, which for homogeneous elements $a, a' \in A$ and $b, b' \in B$, satisfies $\delta(a \otimes b) = \delta(a) + \delta(b)$ and

$$(a \otimes b)(a' \otimes b') = (-1)^{\delta(a)\delta(b)} aa' \otimes bb'.$$

The **graded opposite** A^{grop} is isomorphic to A but with multiplication defined on homogeneous elements $a, b \in A$ via $a^{\mathrm{grop}} b^{\mathrm{grop}} = (-1)^{\delta(a)\delta(b)} (ba)^{\mathrm{grop}}$.

Given a super vector space $V = V_0 + V_1$ over a field K, the endomorphism algebra

$$\mathrm{End}(V) \simeq \underbrace{\mathrm{Hom}(V_0, V_0) + \mathrm{Hom}(V_1, V_1)}_{\text{degree } 0} + \underbrace{\mathrm{Hom}(V_0, V_1) + \mathrm{Hom}(V_1, V_0)}_{\text{degree } 1}$$

is a central simple superalgebra over K

Our presentation of Wall and Clifford invariants leans heavily on [22].

V.2 Brauer-Wall group

The **graded Brauer group** $\mathrm{BW}(K)$ [23], or *Brauer-Wall group*, is the group of equivalence classes (A) of K-superalgebras of the form $A \widehat{\otimes} \mathrm{End}(V_0 + V_1)$ for some super vector space $V_0 + V_1$. The product of two classes is given by $(A) \cdot (B) = (A \widehat{\otimes}_K B)$ and the inverse by $(A)^{-1} = (A^{\mathrm{grop}})$. The ten-fold way arises in this setting, and we will see below that $\mathrm{BW}(\mathbb{C}) \simeq \mathbb{Z}/2$ and $\mathrm{BW}(\mathbb{R}) \simeq \mathbb{Z}/8$.

Since every algebra can be viewed as a superalgebra with only even elements (i.e. with $A = A_0$), the ordinary Brauer group $\mathrm{Br}(K)$ is a subgroup of $\mathrm{BW}(K)$. The corresponding inclusion belongs to an extension

$$1 \to \mathrm{Br}(K) \to \mathrm{BW}(K) \to Q(K) \to 1,$$

of the abelian group $Q(K)$ of extended square classes, itself the extension

$$1 \to K^\times/(K^\times)^2 \to Q(K) \to \mathbb{Z}/2 \to 0$$

of $\mathbb{Z}/2$ by $K^\times/(K^\times)^2$ with multiplication given by $(d, e) \cdot (d', e') = ((-1)^{ee'}dd', e + e')$.

To describe the homomorphism from from $\mathrm{BW}(K)$ to $Q(K)$, first note that if A/K is a central simple superalgebra, then $Z(A)_0 = K1_A$ and $\widehat{Z}(A)_1 = 0$, but there are two possibilties for the odd part $Z(A)_1$:

- A is of **even type** if $Z(A)_1 = 0$, in which case $Z(A_0) = K(z)$ for some $z \in Z(A_0)$ with $z^2 \in K^\times$ and which gives an inner grading, i.e. $za_iz^{-1} = (-1)^i a_i$ for $a_i \in A_i$. In this case, A/K and $A_0/K(z)$ are central simple algebras.
- A is of **odd type** if $Z(A)_1 \neq 0$, in which case $Z(A) = K(z)$ for some $z \in A_1$ with $z^2 \in K^\times$ and for which $A_1 = zA_0$. In this case, A_0/K and $A/K(z)$ are central simple algebras.

Note that $K(z) = K \times K$ whenever $z \in K^\times$, in which case a central simple algebra over $K \times K$ means a direct product of central simple K-algebras. This implies that a central simple graded algebra A/K is not simple as a K-algebra iff it has odd type with $z^2 \in (K^\times)^2$.

The homomorphism $\mathrm{BW}(K) \to Q(K)$ then acts as $(A) \mapsto (d, e)$, where $e \in \{0, 1\}$ is the type of A (even or odd), and where the square class $d = z^2 \bmod (K^\times)^2$ is a well-defined element of $K^\times/(K^\times)^2$ because z is determined up to multiplication by scalars in $K^\times$. The element z appears naturally in the theory of Clifford algebras (e.g. as the fifth gamma matrix), as we see in the next section.

Some authors refer to the **Wall invariants** of a central simple superalgebra A, consisting of its supercenter K and its class in $\mathrm{BW}(K)$, which is determined by the type $e \in \{0, 1\}$ of A(even/odd), the square class of z^2 in $K^\times/(K^\times)^2$ and the ordinary class in $\mathrm{Br}(K)$ of either A/K (in the even case) or of A_0/K (in the odd case).

V.3 Clifford algebras

Let (V, q) be a quadratic space over a field K. The **Clifford algebra** $C(V, q)$ is the quotient of the tensor algebra of V by the ideal generated by the elements $v^2 - q(v)$. The tensor algebra carries a natural $\mathbb{Z}/2$-grading such that this ideal is homogeneous (i.e. is generated by homogeneous elements). Therefore, $C(V)$ inherits this natural $\mathbb{Z}/2$-grading $C(V)_0 \oplus C(V)_1$, which is independent of the characteristic of K and also of the regularity of q. Alternatively, we can define $C(V)$ to be the associative K-algebra generated by the vectors $v \in V$ subject to $v^2 = q(v)$. As a vector space

$$\begin{aligned} C(V) &= \bigoplus_{k=0}^{n} \bigwedge^k V = \bigoplus_{k=0}^{n} \operatorname{span}_K\{v_{i_1} \cdots v_{i_k} : 1 \le i_1 < \cdots < i_k \le n\} \\ &= \operatorname{span}_K\{v_I : I \subset \{1, \ldots, n\}\}, \end{aligned}$$

where, given $I = \{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$ with $i_1 < \ldots < i_k$, we define $v_I := v_{i_1} \cdots v_{i_k}$. The Clifford algebra $C(V)$ can be viewed as a deformation of the exterior algebra $\bigwedge V$, to which it is isomorphic when $q = 0$.

The **grade automorphism** is the K-linear automorphism

$$\alpha(v_1 \cdots v_k) = (-1)^k v_1 \cdots v_k$$

of $C(V)$, which restricts to $(-1)^a$ on $C(V)_a$. The **canonical involution** is the K-linear antiautomorphism

$$(v_1 \cdots v_k)' = v_k \cdots v_1$$

of $C(V)$.

The bilinear form associated to q takes the explicit form

$$b_q(v, x) = q(v + x) - q(v) - q(x) = (v + x)^2 - x^2 - v^2 = vx + xv.$$

For $u \in C(V)^\times$, let $r_u \colon x \mapsto \alpha(u) x u^{-1}$ and note that $r_u r_w = r_{uw}$. Each **anisotropic** $v \in V$ (meaning $q(v) \neq 0$) defines a **transvection**

$$r_v(x) = -vxv^{-1} = (xv - b_q(v, x))v^{-1} = x - b_q(v, x)v^{-1} = x - \frac{b_q(v, x)}{q(v)} v, \qquad \text{(V.1)}$$

where we have used $v^{-1} = \frac{v}{v^2}$

Away from characteristic 2, we can define the bilinear form $b(v, x) = \frac{1}{2} b_q(v, x)$, which satisfies $q(v) = b(v, v)$ and reproduces the familiar formula

$$r_v(x) = x - 2\frac{b(x, v)}{b(v, v)} v \qquad \text{(V.2)}$$

for the **reflection** through the subspace perpendicular to v, for which $r_v(v) = -v$ and $r_v(w) = w$ if $b_q(v, w) = 0$.

V.4 The Clifford invariant

Let (V, q) be a nondegenerate quadratic space over a field K (of characteristic not equal to 2, for simplicity). The Clifford algebra $C(q)$ has a canonical grading making it a central simple K-superalgebra. Given another nondegenerate quadratic space (V', q') over K, we have $C(q \oplus q') = C(q)\widehat{\otimes}_K C(q')$ and $C(-q) = C(q)^{\mathrm{grop}}$. Therefore the image of $C(q)$ in $\mathrm{BW}(K)$ is an invariant of (V, q) – the **Clifford invariant** – while the associated map factors through the **Witt group** $W(K)$ of isometry classes $[(V, q)]$ of the anisotropic parts of quadratic spaces (V, q) over K with group structure

$$[(V, q)] + [(V', q)] = [(V \oplus V', q \oplus q')] \text{ and } [(V, q)]^{-1} = [(V, -q)].$$

Let $e_1, \ldots, e_n$ be an orthogonal basis for (V, q) and let $z = e_1 \cdots e_n$. Then $z^2 \in K^\times$ and the image of z^2 modulo $(K^\times)^2$ is equal to the **discriminant** (following e.g. [6] Definition 2.1) or "signed determinant" [22]

$$\mathrm{disc}(V) := (-1)^{n(n-1)/2} \det(V) = \begin{cases} \det(V) & \text{if } \dim(V) \equiv 0 \text{ or } 1 \bmod 4 \\ -\det(V) & \text{if } \dim(V) \equiv 2 \text{ or } 3 \bmod 4, \end{cases}$$

where $\det(V) := \det(q(v_i, v_j)) \bmod (K^\times)^2$ is the square class of the determinant of the Gram matrix of any basis v_i of V, and where $q(v, w) = \frac{1}{2}(q(v + w) - q(v) - q(w))$. The quadratic extension $K(z) \simeq K[x]/(x^2 - \mathrm{disc}(V))$ is therefore well-defined and is isomorphic to either $K \times K$ or a quadratic field extension depending on whether $\mathrm{disc}(V)$ is a square in $K^\times$. We have

$$Z(C(V)) = \begin{cases} K & \text{if } n \text{ is even} \\ K(z) & \text{if } n \text{ is odd,} \end{cases} \quad Z(C(V)_0) = \begin{cases} K(z) & \text{if } n \text{ is even} \\ K & \text{if } n \text{ is odd,} \end{cases}$$

One can also show that $C(V)$ is a central simple K-algebra when $\dim(V)$ is even and $C(V)_0$ is a central simple K-algebra when $\dim(V)$ is odd. If $\mathrm{disc}(V)$ is not a square, then $C(V)_0$ is a central simple $K(z)$-algebra when n is even and $C(V)$ is a central simple $K(z)$-algebra when n is odd. If $\mathrm{disc}(V)$ is a square, then $C(V)_0$ is the direct product of two central simple K-algebras when n is even and $C(V)$ is the direct product of two central simple K-algebras when n is odd. Despite all this complexity

$$\widehat{Z}(C(V)) = \widehat{Z}(C(V)_0) = Z(C(V)_0) = K$$

verifies that in every dimension, $C(V)$ is a central simple K-superalgebra.

V.5 Brauer-Wall groups over $\mathbb{R}$

$$1 \to \underbrace{\mathrm{Br}(\mathbb{C})}_{1} \to \underbrace{\mathrm{BW}(\mathbb{C})}_{\mathbb{Z}/2} \to \underbrace{Q(\mathbb{C})}_{\mathbb{Z}/2} \to 1$$

where $Q(\mathbb{C}) = \mathbb{Z}/2$ is the trivial extension

$$1 \to \underbrace{\mathbb{C}^\times/(\mathbb{C}^\times)^2}_{1} \to \underbrace{Q(\mathbb{C})}_{\mathbb{Z}/2} \to \langle -1\rangle \to 1.$$

Over $\mathbb{R}$, we have the exact sequence

$$1 \to \underbrace{\mathrm{Br}(\mathbb{R})}_{\mathbb{Z}/2} \to \underbrace{\mathrm{BW}(\mathbb{R})}_{\mathbb{Z}/8} \to \underbrace{Q(\mathbb{R})}_{\mathbb{Z}/4} \to 1$$

where

$$1 \to \underbrace{\mathbb{R}^\times/(\mathbb{R}^\times)^2}_{\mathbb{Z}/2} \to \underbrace{Q(\mathbb{R})}_{\mathbb{Z}/4} \to \langle -1\rangle \to 1.$$

V.5.1 The 10-fold way

Let V be a complex vector space with a nondegenerate Hermitian form $h\colon V \times V \to \mathbb{C}$ and let $J \in \mathrm{Aut}_{\mathbb{R}}(\mathrm{End}(V))$ be the corresponding involution for which $h(v, aw) = h(J(a)v, w)$ for every $a \in \mathrm{End}(V)$ and every $v, w \in V$. Given a Hamiltonian $H \in \mathrm{End}(V)^{\langle J\rangle}$, i.e. H is Hermitian, satisfying $J(H) = H$, its symmetry group $\mathrm{End}_{\mathbb{R}}(V)^H = \{g \in \mathrm{End}_{\mathbb{R}}(V) : gHg^{-1} = H\}$ decomposes into a unitary part and a possible antiunitary part. Antiunitary symmetries include time-reversal or charge conjugation. On the other hand, given a unitary representation of a group G, we can ask for the space $\mathrm{End}(V)^J \cap \mathrm{End}(V)^G = \mathrm{End}(V)^{\langle J,G\rangle}$ of Hermitian operators commuting with the action of G.

V.6 Superalgebras over involuted fields

Wall further considered involuted superalgebras (A, J), where A is a central simple superalgebra over K with involution J restricting to j on the center $Z(A)$ [21]. The grading on A determines a second involution J' on A such that $J'(a) = (-1)^i J(a)$ if $a \in A_i$. Because $Z(A)_0 = \widehat{Z}(A) = K$, these involutions coincide on the even part A_0 and, in particular, on the graded center $\widehat{Z}(A)$. If A is of even type, then they coincide on the ordinary center $Z(A)$, but if A is of odd type, they differ on the odd part of the center.

There is a 54-fold way of Brauer groups associated to the involuted fields extending $\mathbb{R}$:

$$1 \to \underbrace{\mathrm{BW}(\mathbb{R}, 1)}_{\mathbb{Z}/8\times\mathbb{Z}/4} \to \underbrace{\mathrm{BW}(\mathbb{C}, 1)}_{\mathbb{Z}/8} \times \underbrace{\mathrm{BW}((\mathbb{R}\times\mathbb{R})/\mathbb{R}, s)}_{\mathbb{Z}/8} \to \underbrace{\mathrm{BW}((\mathbb{C}\times\mathbb{C})/\mathbb{C}, s)}_{\mathbb{Z}/2} \to 1.$$

Chapter VI
Orthogonal and spin groups

VI.1 The Clifford group

Let (V, q) be a quadratic space. The **Clifford group**[1]

$$\mathrm{GPin}(V) = \{u \in C(V,q)^\times : r_u(V) = V\} \subset C(V,q)_h^\times$$

is the subgroup of homogeneous units in the Clifford algebra taking V to itself. It is an extension

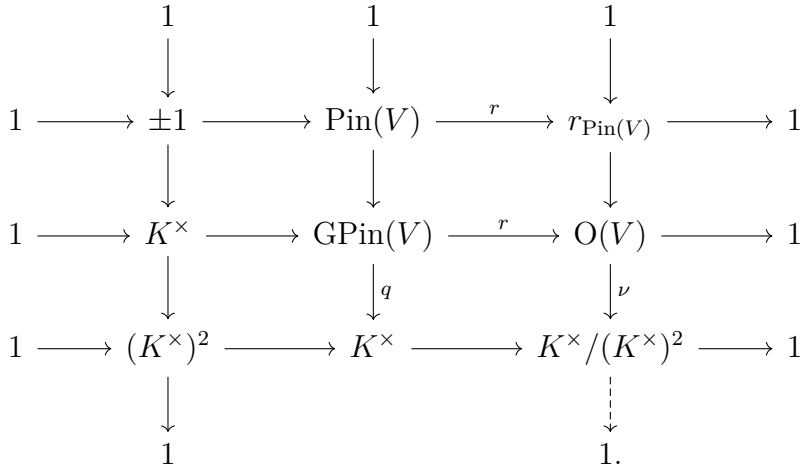
$$1 \to K^\times \to \mathrm{GPin}(V) \xrightarrow{r} \mathrm{O}(V) \to 1$$

of the orthogonal group $O(V)$. The quadratic form q extends to a homomorphism $q\colon \mathrm{GPin}(V) \to K^\times$ known as the **Clifford norm** $q(u) = u'u$. Let $\mathrm{Pin}(V)$ be its kernel. The **spinor norm**

$$\nu\colon \mathrm{O}(V) \to K^\times/(K^\times)^2$$

is the map induced by the Clifford norm via $\nu(r_u) = q(u)(K^\times)^2$ (following [6] on the sign).

We follow [6] (Section 9.§3) by organizing the relevant groups into the following diagram with exact rows and columns; the dotted arrow is included when V is isotropic:



[1]The Clifford group was never actually defined by Clifford, but was instead introduced by Lipschitz. Also not the same as the Clifford group of quantum information theory although it is somewhat related over $\mathbb{F}_2$. Clifford algebras had been called Clifford-Lipschitz algebras until Chevalley started calling them Clifford algebras in the 50s. See [24], [25] for more on this history.

VI.2 Special orthogonal and spin group

Because its elements are homogeneous, the Clifford group decomposes as a disjoint union $\mathrm{GPin}(V) = \mathrm{GPin}(V)_0 \cup \mathrm{GPin}(V)_1$ with $\mathrm{GPin}(V)_i := \mathrm{GPin}(V) \cap C(V)_i$. Define

$$\begin{aligned} \mathrm{GSpin}(V) &:= \mathrm{GPin}(V)_0 \\ \mathrm{SO}(V) &:= r_{\mathrm{GSpin}(V)} \\ \mathrm{Spin}(V) &:= \mathrm{Pin}(V) \cap C(V)_0 = \ker q|_{\mathrm{GSpin}(V)} \\ \Theta(V) &:= r_{\mathrm{Spin}(V)} \end{aligned}$$

and note that $[\mathrm{O}(V) : \mathrm{SO}(V)] = 2$ in every characteristic[2]. The previous diagram becomes

$$\begin{array}{ccccccccc} & & 1 & & 1 & & 1 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \pm 1 & \longrightarrow & \mathrm{Spin}(V) & \xrightarrow{r} & \Theta(V) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & K^\times & \longrightarrow & \mathrm{GSpin}(V) & \xrightarrow{r} & \mathrm{SO}(V) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow q & & \downarrow \nu & & \\ 1 & \longrightarrow & (K^\times)^2 & \longrightarrow & K^\times & \longrightarrow & K^\times/(K^\times)^2 & \longrightarrow & 1 \\ & & \downarrow & & & & \vdots & & \\ & & 1 & & & & 1 & & \end{array}$$

Given $g, h \in \mathrm{O}(V)$, note that $ghg^{-1}h^{-1} \in \mathrm{SO}(V)$ and

$$\nu(ghg^{-1}h^{-1}) = \nu(g)\nu(h)\nu(g)^{-1}\nu(h)^{-1} = 1.$$

Therefore $[\mathrm{O}(V), \mathrm{O}(V)] \subset \Theta(V)$ and we have a subnormal series

$$\mathrm{O}(V) \supset \Theta(V) \supset [\mathrm{O}(V), \mathrm{O}(V)] \supset [\mathrm{SO}(V), \mathrm{SO}(V)] \supset \{I\}. \tag{VI.1}$$

The spinor norm is surjective if V is isotropic, in which case $\mathrm{SO}(V)$ is an extension

$$1 \to \Theta(V) \to \mathrm{SO}(V) \to K^\times/(K^\times)^2 \to 1$$

of the full group $K^\times/(K^\times)^2$ of square classes by the image $\Theta(V)$ of the spin group $\mathrm{Spin}(V)$. Because $(K^\times)^p = K^\times$ iff K is perfect of characteristic p, the group $K^\times/(K^\times)^2$ of square classes is trivial iff K is perfect of characteristic 2. In such a case, the spinor norm is trivially surjective and we have $\mathrm{SO}(V) = \Theta(V) \simeq \mathrm{Spin}(V)$.

[2]Note that we do **not** define $\mathrm{SO}(V)$ as the kernel of the determinant map on $\mathrm{O}(V)$. Chevalley calls this group O^+. It can also be defined by modifying the determinant [2], [5].

Theorem VI.2.1 Let V be an isotropic quadratic space. There are three possibilities

- $\dim(V) = 2$, in which case $\mathrm{SO}(V)$ is abelian, $\Theta(V) = [\mathrm{O}(V), \mathrm{O}(V)]$ and $[\mathrm{SO}(V), \mathrm{SO}(V)] = \{I\}$.
- V is a 4d hyperbolic space H over $\mathbb{F}_2$.
- Otherwise $\Theta(V) = [\mathrm{O}(V), \mathrm{O}(V)] = [\mathrm{SO}(V), \mathrm{SO}(V)]$

For a proof see e.g. Section 6 of [26].

The isometry group

$$\mathrm{O}(H) \simeq \mathrm{O}_{2,2}(\mathbb{F}_2) \simeq (\mathrm{SL}_2(\mathbb{F}_2) \times \mathrm{SL}_2(\mathbb{F}_2)) \rtimes \mathbb{Z}/2$$

of the 4d hyperbolic space H over $\mathbb{F}_2$ is an index-10 subgroup of the symplectic group $\mathrm{Sp}_4(\mathbb{F}_2)$. Its commutator subgroup is

$$[\mathrm{O}(H), \mathrm{O}(H)] \simeq (\mathbb{Z}/3 \times \mathbb{Z}/3) \rtimes \mathbb{Z}/2.$$

Together with any local transposition, it generates $\mathrm{SO}(H)$, for which $[\mathrm{SO}(H), \mathrm{SO}(H)] \simeq \mathbb{Z}/3 \times \mathbb{Z}/3$, giving a subnormal series with orders 72, 36, 18 and 9.

The hyperbolic space H is exceptional in another way:

Theorem VI.2.2 (Cartan-Dieudonne Theorem) Let V be a quadratic space with $V \not\simeq H$. Then $\mathrm{O}(V)$ is generated by the r_v for non-isotropic $v$each element being the product of at most $\dim(V)$ such transvections.

The subgroup of $\mathrm{O}(H)$ generated by transvections contains $\mathrm{SL}(2) \times \mathrm{SL}(2)$ because $q_{11} \oplus q_{11}$ is anisotropic. Identifying these as a subgroup of local Cliffords, it must be that the SWAP is not a transvection, so that the transvection subgroup is equal to $\mathrm{SL}(2) \times \mathrm{SL}(2)$. Interestingly, one can show that this most basic qubit SWAP gate cannot be built from transvections unless there are at least 3 qubits. Actually it has trivial Dickson invariant (so is contained in $\mathrm{SO}(q \oplus q)$), implying it is not a transvection as $\Delta(r_v) = 1$ for isotropic v. One implication of this is that there is an inclusion $S_n \hookrightarrow \mathrm{SO}(q^{\oplus n})$ for every nondegenerate quadratic form $q : \mathbb{F}_2^2 \to \mathbb{F}_2$.

Computations in Magma confirm that $|O(B)| = |\mathrm{Sp}_4(2)| = 720$, whereas

$$|\mathrm{O}(q \oplus q')| = \begin{cases} 72 & \text{if } \mathrm{Arf}(q) = \mathrm{Arf}(q') \\ 120 & \text{if } \mathrm{Arf}(q) \neq \mathrm{Arf}(q'). \end{cases}$$

Each $\mathrm{O}(q \oplus q')$ is its own normalizer in $\mathrm{Sp}_4(\mathbb{F}_2)$. I think this means that each left coset is a right coset and vice-versa, so the double cosets are diagonal. Furtherore, $\mathrm{O}(q \oplus q')$ and $\mathrm{O}(p \oplus p')$ are conjugate in $\mathrm{Sp}_4(\mathbb{F}_2)$ iff they have the same Arf invariant.

There is a lot of annoyingly conflicting notation in the literature, even more confusing since many of the relevant subgroups coincide in most cases.

	grading	$\det=1$	Γ	$\mathrm{im}(\Gamma_0)$	$q\|_{\Gamma_0}=1$	im(Spin)	commutator
Here	$0/1$		Γ	SO	Spin	$r(\mathrm{Spin})$	$[\mathrm{O},\mathrm{O}]$
Chevalley	$\pm$		Γ	O^+	Γ_0^+	Ω	O'
Cassels	$0/1$	O^+	Γ		Spin	Θ	Ω
O'Meara	$\pm$	O^+				O'	Ω
Borcherds	$0/1$		Γ	SO	Spin		

VI.3 Real orthogonal groups

Let $V = \mathbb{R}^{m+n}$ and take

$$q(x) = x^T \operatorname{diag}(1, \dots, 1, -1, \dots, -1)x = x_1^2 + \cdots + x_m^2 - x_{m+1}^2 - \cdots - x_{m+n}^2.$$

If $m, n \geq 1$, then $\mathrm{O}_{m,n}(\mathbb{R})$ has four connected components

$$\mathrm{O}_{m,n}(\mathbb{R}) = \mathrm{O}_{m,n}(\mathbb{R})^{00} \cup \mathrm{O}_{m,n}(\mathbb{R})^{01} \cup \mathrm{O}_{m,n}(\mathbb{R})^{10} \cup \mathrm{O}_{m,n}(\mathbb{R})^{11},$$

where $\mathrm{O}_{m,n}(\mathbb{R})^{ij}$ changes the orientation on the first m coordinates by $(-1)^i$ and on the second n by $(-1)^j$. This can be shown using a Clifford algebra represented on $\bigwedge^m \mathbb{R}^m \otimes \bigwedge^n \mathbb{R}^n$.

For example,

$$\mathrm{O}_{1,1}(\mathbb{R})^{00} = \left\{ \begin{pmatrix} \cosh(a) & \sinh(a) \\ \sinh(a) & \cosh(a) \end{pmatrix} : a \in \mathbb{R} \right\}.$$

The special orthogonal group has two connected components

$$\mathrm{SO}_{m,n}(\mathbb{R}) = \mathrm{SO}_{m,n}(\mathbb{R})^0 \cup \mathrm{SO}_{m,n}(\mathbb{R})^1 = \mathrm{O}_{m,n}(\mathbb{R})^{00} \cup \mathrm{O}_{m,n}(\mathbb{R})^{11}.$$

The spinor norm is constant on the connected components and so can be computed on any element. Its kernel is

$$\Theta_{m,n}(V) = \mathrm{O}_{m,n}(\mathbb{R})^{00} = \mathrm{SO}_{m,n}(\mathbb{R})^0.$$

When m and n are odd there are canonical choices for "time reversal"

$$T = r_{\mathbf{x}_1} \cdots r_{\mathbf{x}_m} = \operatorname{diag}(-1, \dots, -1, 1 \dots, 1) \in \mathrm{O}_{m,n}(\mathbb{R})^{10},$$

for "parity-reversal"

$$P = r_{\mathbf{x}_{m+1}} \cdots r_{\mathbf{x}_{m+n}} = \operatorname{diag}(1, \dots, 1, -1, \dots, -1) \in \mathrm{O}_{m,n}(\mathbb{R})^{01}$$

and for "charge-conjugation"

$$C = TP = r_{\mathbf{x}_1} \cdots r_{\mathbf{x}_{m+n}} = \operatorname{diag}(-1, \dots, -1).$$

If m is even then one of the first reflections needs to be dropped, and similarly with n (but there is no canonical choice). This means an odd number of reflections is needed to change orientation, so that $\nu(r_{\mathbf{x}_1}) = 1$ and $\nu(r_{\mathbf{x}_{m+1}}) = -1$, implying that $\nu(T) = 1$ and $\nu(P) = \nu(C) = -1$.[3]

$r(\mathrm{Spin}_{m,n}(\mathbb{R})) = [\mathrm{O}_{m,n}(\mathbb{R}), \mathrm{O}_{m,n}(\mathbb{R})]$ is the connected component of $\mathrm{O}_{m,n}(\mathbb{R})$ containing the identity.

[3]Unless you're on the East coast or using the other sign convention for the spinor norm, in which case $\nu(T) = -1$ and $\nu(P) = 1$.

If $n = 0$ then there are only two components

$$\mathrm{O}_{m,0}(\mathbb{R}) = \mathrm{O}_{m,0}(\mathbb{R})^0 \cup \mathrm{O}_{m,0}(\mathbb{R})^1$$

and $\nu = 1$ on both components whereas $\det(\mathrm{O}_{m,0}(\mathbb{R})^i) = (-1)^i$. In particular, $\mathrm{SO}_{m,0}(\mathbb{R}) = \mathrm{O}_{m,0}(\mathbb{R})^0$. If $m = 0$ we similarly have

$$\mathrm{O}_{0,n}(\mathbb{R}) = \mathrm{O}_{0,m}(\mathbb{R})^0 \cup \mathrm{O}_{0,n}(\mathbb{R})^1$$

in which case $\nu(\mathrm{O}_{0,n}(\mathbb{R})^i) = \det(\mathrm{O}_{0,n}(\mathbb{R})^i) = (-1)^n$. So over the reals, the spinor norm is only interesting in the indefinite case.

In lower dimensions, we have

$\mathbb{R}^\times \simeq \mathbb{R}^+ \times \{\pm 1\}$ and $\mathrm{SO}_{1,1}(\mathbb{R}) \simeq \mathbb{R}^+$.

VI.4 Characteristic 2

> The properties of $\mathbb{Q}_2$-valued forms under $\mathbb{Z}_2$-equivalence are really rather tiresome. Fortunately... a detailed knowledge is not needed for the discussion of "global" forms. Only the masochist is invited to read this section.
>
> (J.W.S. Cassels, Section 8.2 of *Rational Quadratic Forms* [4])

> With the preservation of his sanity uppermost on his mind, this senior-aged author has made his clear and unequivocal choice. Unless explicitly stated to the contrary, *all fields over which quadratic forms are considered in this book will be assumed to have characteristic not equal to 2.*
>
> (T.Y. Lam, *Introduction to Quadratic Forms over Fields* [22])

> I prefer to stick to even unimodular lattices. Life is too short to figure out exactly what happens at the prime 2 for general quadratic forms.
>
> (some Fields medalist)

> Not only was Jacques Tits a constant source of inspiration through his work, but he also had a direct personal influence, notably through his threat — early in the inception of our project — to speak evil of our work if it did not include the characteristic 2 case. Finally he also agreed to bestow his blessings on our book sous forme de préface.
>
> (Introduction to *The Book of Involutions [2]*)

One cannot always avoid characteristic 2. Applications to coding theory largely involve binary codes. Characteristic 2 arises naturally when reducing by appropriate primes. The group $F^\times/(F^\times)^2$ of square classes of each completion F of $\mathbb{Q}$ is a vector space over $\mathbb{F}_2$, having dimension 1 for $\mathbb{R}$, dimension 2 for $\mathbb{Q}_p$ with odd p and dimension 3 for $\mathbb{Q}_2$.

Given a quadratic form $q : V \to K$, let $V^\perp = \{v \in V : b_q(v, V) = 0\}$. We follow [2] and call q **regular** if either $V^\perp = 0$, or $\dim(V^\perp) = 1$ and $q(V^\perp) \neq 0$, with the latter case only occuring for odd-dimensional spaces in characteristic 2. Some authors [5] (p. 207) call the latter case *semiregular*.

Let (V, q) be an even-dimensional regular quadratic space over a field K of characteristic 2. Then V has a **symplectic basis** $e_1, f_1, \ldots, e_n, f_n$ with respect to which

$$q(x) = x^T \begin{pmatrix} a_1 & 1 & & & \\ & b_1 & & & \\ & & \ddots & & \\ & & & a_n & 1 \\ & & & & b_n \end{pmatrix} x = \tilde{x}^T \begin{pmatrix} a_1 & & & 1 & & \\ & \ddots & & & \ddots & \\ & & a_n & & & 1 \\ & & & b_1 & & \\ & & & & \ddots & \\ & & & & & b_n \end{pmatrix} \tilde{x}$$

where $a_i = q(e_i)$, $b_i = q(f_i)$ and $\tilde{x} = (x_1, x_3, \ldots, x_{2n-1}, x_2, x_4, \ldots, x_{2n})^T$. The associated bilinear form is then

$$B_q(x,y) = x^T \begin{pmatrix} & 1 & & & \\ 1 & & & & \\ & & \ddots & & \\ & & & & 1 \\ & & & 1 & \end{pmatrix} y = \tilde{x}^T \begin{pmatrix} & & & 1 & \\ & & & & \ddots \\ & & & & & 1 \\ 1 & & & & \\ & \ddots & & & \\ & & 1 & & \end{pmatrix} \tilde{y},$$

so we see there is, up to basis changes, only one regular bilinear form on an even-dimensional vector space in characteristic 2.

The orthogonal group $\mathrm{O}(V)$ acts as automorphisms of $C(V)$, fixing $C(V)_0$ and $Z(C(V)_0)$ setwise. Since $Z(C(V)_0)$ is a separable quadratic extension of K, its automorphism group over K is isomorphic to $\mathbb{Z}/2$, so the action of $\mathrm{O}(V)$ on $Z(C(V)_0)$ defines a homomorphism $\mathrm{O}(V) \to \mathbb{Z}/2$ called the **Dickson invariant**, whose kernel is precisely $\mathrm{SO}(V)$.

Note that the subset $\wp(K) = \{x + x^2 : x \in K\}$ is an additive subgroup of K because

$$(x+y) + (x+y)^2 = x + y + x^2 + 2xy + y^2 = x + x^2 + y + y^2.$$

The **Arf invariant** $\mathrm{Arf}(q)$ is the image of $\sum_i a_i b_i$ in the additive group $K/\wp(K)$, The Artin-Schreier isomorphism $K/\wp(K) \simeq H^1(K, \mathbb{F}_2)$ gives a 1-1 correspondence between the group $K/\wp(K)$ and the separable quadratic extensions of K (see [6] p. 313). For example, $\wp(\mathbb{F}_2) = 0$, so there are two separable quadratic extensions of $\mathbb{F}_2$: $\mathbb{F}_4$ and $\mathbb{F}_2 \times \mathbb{F}_2$.

In characteristic 2, the orthogonal group $O(q)$ is generated by the **transvections** $r_v(w) = w + \frac{B_q(w,v)}{q(v)} v$ defined by the anisotropic v (i.e. for which $q(v) \neq 0$). Transvections are characteristic-2 analogs of reflections $w \mapsto w + \frac{B_q(x,v)}{2q(v)}$. Because $\frac{B_q(v,v)}{q(v)} = 2$ for nonisotropic v, transvections satisfy $r_v(v) = v$ (as do reflections), but they do something other than negate orthogonal vectors (because $-1 = 1$ in characteristic 2).

For $a, b \in \mathbb{F}_2$, let

$$q_{ab}(x) = x^T \left(\begin{smallmatrix} a & 1 \\ 0 & b \end{smallmatrix}\right) x = ax_1^2 + x_1x_2 + bx_2^2.$$

All four of these quadratic forms have the same associated bilinear form $B_{q_{11}} = x^T \left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right) y = x_1y_2 + x_2y_1$.

The quadratic form $q_{11}(x) = x_1^2 + x_1x_2 + x_2^2$ is the unique anisotropic form on $\mathbb{F}_2^2$. Because $q_{11}(\mathbb{F}_2^2 \setminus 0) = 1$, each of the three nonzero vectors in $\mathbb{F}_2^2 \setminus 0 = \left\{ \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \right\}$ defines an $r_v \in O(q_{11})$, which fixes v while swapping the other two vectors. Therefore $\mathrm{O}(q_{11}) \simeq S_3 \simeq \mathrm{SL}_2(\mathbb{F}_2)$. Furthermore,

$$\mathrm{SO}(q_{11}) = \Theta(q_{11}) = [\mathrm{O}(q_{11}), \mathrm{O}(q_{11})] = \left\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \right\rangle \simeq \mathbb{Z}/3$$

and $[\mathrm{SO}(q_{11}), \mathrm{SO}(q_{11})]$ is trivial. Note that $\mathrm{SO}(q_{11})$ preserves the matrix $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, while the orbit of the full $\mathrm{O}(q_{11})$ consists of $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and its transpose $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$, each of which give rise to the same quadratic form q_{11}. The Arf invariant is $\Delta(q_{11}) = 1 \in \mathbb{F}_2$. The associated bilinear form $B_{q_{11}} = x^T\left(\begin{smallmatrix}&1\\1&\end{smallmatrix}\right)y = x_1y_2 + x_2y_1$ has the same automorphism group as $\mathrm{O}(q_{11})$.

The remaining three quadratic forms q_{00}, q_{01} and q_{10} are isotropic and make up a single equivalence class. They all have trivial Arf invariant, so the Arf invariant distinguishes the two equivalence classes (even though both classes have the same associated bilinear form). The automorphism groups of these isotropic forms are

$$\mathrm{O}(q_{00}) = \langle r_{11}\rangle = \left\langle \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\right\rangle, \quad \mathrm{O}(q_{10}) = \langle r_{10}\rangle = \left\langle \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\right\rangle, \quad \mathrm{O}(q_{01}) = \langle r_{01}\rangle = \left\langle \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\right\rangle,$$

which are all isomorphic to $\mathbb{Z}/2$, whereas SO, $\Theta, [\mathrm{O},\mathrm{O}]$ and $[\mathrm{SO},\mathrm{SO}]$ are all trivial. Relation to the theta functions θ_{ab} via $\Gamma_{ab}/\Gamma(2) \subset \mathrm{SL}_2(2)$. Connection to modular forms of half-integral weight / free fermions.

The only counterexample to Cartan-Dieudonne is the hyperbolic space $(\mathbb{F}_2^4, q_{11} \oplus q_{11})$, for which

$$\mathrm{O}(V) = \mathrm{SL}_2(2) \wr \mathbb{Z}/2 = (\mathrm{SL}_2(2) \times \mathrm{SL}_2(2)) \rtimes \mathbb{Z}/2 = \left\langle \left(\begin{smallmatrix}g_1&0\\0&g_2\end{smallmatrix}\right), \left(\begin{smallmatrix}0&I\\I&0\end{smallmatrix}\right) : g \in \mathrm{SL}_2(2)\right\rangle.$$

The subgroup generated by transvections in vectors in $\mathbb{F}_2^2 \oplus 0 \cup 0 \oplus \mathbb{F}_2^2$ is $\mathrm{SL}_2(2) \times \mathrm{SL}_2(2)$. Because all other nonzero vectors in $\mathbb{F}_2^4$ are isotropic, there is no other vector through which we can reflect to get the automorphism swapping the copies of $\mathrm{SL}_2(2)$.

VI.5 Unitary groups

A Hermitian form $\langle \cdot, \cdot \rangle \colon V \times V \to \mathbb{C}$ on a complex vector space V gives rise to a quadratic form $q \colon V \to \mathbb{R}$ via $q(v) = \langle v, v \rangle = v^\dagger v$, where $v^\dagger \in V^*$ is the conjugate transpose with respect to the Hermitian form. So $v^2 = v^\dagger v$ as an element of the corresponding Clifford algebra. The unitary group is the subgroup of the orthogonal group $\mathrm{O}(q)$ preserving either a complex structure or a symplectic form. Keep in mind that Clifford algebras by themselves are used to deal with bilinear forms and orthogonal groups. Unitary groups must additionally preserve either a complex structure or a symplectic form. More precisely, the unitary group satisfies the "two-out-of-three" property

$$\mathrm{U}_n(\mathbb{C}) = \mathrm{O}_{2n}(\mathbb{R}) \cap \mathrm{Sp}_{2n}(\mathbb{R}) \cap \mathrm{GL}_n(\mathbb{C})$$

where the intersection of any two is contained in the third.

Chapter VII
Integrality

VII.1 R-lattices

Let R be an integral domain with fraction field K. An R-module M is **torsion free** if whenever $r \in R$ and $m \in M$ satisfy $rm = 0$, then either $r = 0$ or $m = 0$. Equivalently, M is torsion free if the natural map from M into the vector space $M_K := K \otimes_R M$ is injective.

Exercise VII.1.1 Show that a commutative ring is an integral domain iff it is a torsion-free module over itself.

An **R-lattice** is a finitely generated torsion-free R-module. The **rank** $\mathrm{rank}_R(\Lambda) = \dim_K(\Lambda_K)$ of an R-lattice Λ is the maximum number of linearly independent elements of Λ. By an R-lattice in a finite-dimensional vector space V/K, we mean an R-lattice Λ generated by a basis for V ([1] calls this a *full R-lattice*). Every R-lattice over a Dedekind domain is projective and every R-lattice over a PID is free. Over an integrally closed Noetherian domain, each R-lattice Λ is an extension

$$0 \to R^n \to \Lambda \to \mathfrak{a} \to 0,$$

of some ideal $\mathfrak{a} \subset R$ by a free R-module. By definition, this sequence only splits to give $\Lambda \simeq R^n \oplus \mathfrak{a}$ when $\mathfrak{a}$ is projective. Over a Noetherian domain, the torsion-free requirement means $\mathrm{Ass}(\Lambda) = (0)$, while over a Noetherian ring, $\mathrm{Ass}(M) \subset \mathrm{Ass}(\Lambda)$, where $\mathrm{Ass}(M)$ is the set of prime ideals $\mathfrak{p} \subset R$ that equal the annihilator of some element of Λ.

VII.2 Integral R-algebras

Let R be an integral domain. An element a in an R-algebra is **integral** if there exists a monic polynomial $f \in R[x]$ such that $f(a) = 0$, i.e. if there are $r_i \in R$ such that $a^n + r_{n-1}a^{n-1} + \cdots + r_0 = 0$. The **integral closure** of R in A is the set of elements of A that are integral over R. One would in principle need to check all monic polynomials vanishing at a to decide whether a is R-integral. However, if R is an integrally closed domain with fraction field K, then ([1] 1.14) an element a of an R-algebra is integral iff its minimal polynomial over K is contained in $R[x]$.

Theorem VII.2.1 Let A be a commutative algebra over an integral domain R. Then the integral closure of R in A is a ring, hence an R-algebra.

The proposition follows directly from two lemmas:

Lemma VII.2.1 (c.f. [1] Theorem 1.10) Every finitely generated algebra over an integral domain is integral.

Proof. Let A be a finitely generated algebra over an integral domain R. Since A is finitely generated over R, it has an integral basis a_i such that $A = Ra_1 + \cdots + Ra_n$. Because A is a ring, left multiplication by $a \in A$ transforms this basis according to a matrix $\alpha \in R^{n\times n}$ such that $aa_i = \sum_j \alpha_{ij} a_j$. This implies that

$$0 = \det(aI_m - \alpha) = a^n + r_{n-1}a^{n-1} + \cdots + r_0$$

with each $r_i \in R$, hence a is integral. □

Lemma VII.2.2 Let A be an algebra over a commutative ring R and let $a, b \in A$ be integral elements that commute. Then $R[a, b]$ is a finitely generated over R.

Proof. By commutativity, integrality and associativity (in that order),

$$R[a,b] = R[a]R[b] = \left(\sum_{i=1}^{n} Ra^i\right)\left(\sum_{j=1}^{m} Rb^j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} Ra^i b^j.$$

Therefore $R[a, b]$ is finitely generated as an R-module. □

Proof of Proposition. Let $a, b \in A$ be arbitrary. Because they commute, $R[a, b]$ is a finitely generated R-module by Lemma VII.2.1. By Lemma VII.2.2, a, b, $a \pm b$ and ab are all integral since they are contained in $R[a, b]$. The theorem follows. □

The theorem fails in the noncommutative case. For example, let $R = \mathbb{Z}$, $F = \mathbb{Q}$, $A = \mathbb{Q}^{2\times 2}$. Then $a = \left(\begin{smallmatrix} 0 & 1/2 \\ 0 & 0 \end{smallmatrix}\right)$ and $b = \left(\begin{smallmatrix} 0 & 0 \\ 1/2 & 0 \end{smallmatrix}\right)$ are elements of A that are integral over $\mathbb{Z}$ because $a^2 = b^2 = 0$, but $a + b$ is not integral because its characteristic polynomial is $x^2 - 1/4$. On the other hand, $\mathbb{Z}[a, b] = \mathbb{Z}[\frac{1}{2}]^{2\times 2}$ is integral over the Dedekind domain $\mathbb{Z}[\frac{1}{2}]$, so Theorem VII.2.1 holds if we take $R = \mathbb{Z}[\frac{1}{2}]$. So this is not much different than picking $a = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and $b = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, in which case $\mathbb{Z}[a, b] = \mathbb{Z}^{2\times 2}$ is integral over $\mathbb{Z}$.

VII.2.1 R-orders

Let R be an integral domain with fraction field K and let A be a finite-dimensional K-algebra. An R-**order** in A is a finitely generated torsion-free R-subalgebra $\Lambda \subset A$ with $\Lambda_K = A$, i.e. an R-lattice in A that is also a ring.

Proposition ([1] 8.6). *Every R-order is R-integral. If R is integrally closed in K, then the minimum polynomial and characteristic polynomial of each element in an R-order is contained in $R[x]$.*

Every element of an R-order is R-integral, every R-integral element is contained in some R-order, and every R-order is contained in some maximal R-order. When A is a separable commutative F-algebra, then A contains a unique maximal R-order; for example, the maximal $\mathbb{Z}$-order in a number field is its ring of integers. Nonseparable commutative algebras need not contain any maximal orders (see p. 110 of [1]).

The integral closure of R in A is the union of all maximal orders, and unless A is commutative, the integral closure may not be closed under addition. Maximal orders are therefore the correct generalizations of rings of integers to the noncommutative case. Noncommutative rings generally contain infinitely many maximal orders, partitioned into finitely many conjugacy classes.

VII.3 Twisted trace form, discriminant and different

Let R be an integrally closed Noetherian domain that is not a field and let A be a semisimple algebra over the fraction field K of R. Let O be an R-order of A. Because R is a Noetherian integrally closed domain, the reduced characteristic polynomial of any element $a \in \Lambda$ is contained in $R[x]$ and in particular, its reduced norm and reduced trace are in R. Because ab is integral whenever a and b are, the trace form restricts to a nondegenerate bilinear symmetric form $T\colon \Lambda \times \Lambda \to R$.

Given an involution σ on A and a $u \in A^\times$ fixed by σ, the **twisted trace form**

$$T_{(\sigma,u)}(x,y) = \mathrm{Trd}(\sigma(x)uy)$$

is nonsingular iff u is invertible. If A is central simple it is a symmetric bilinear form when if σ is of the first kind and a hermitian form if σ is of the second kind. If σ stabilizes an R-lattice Λ, then $T_{(\sigma,1)}$ is integral on Λ iff Λ is an order.

If $\Lambda^\vee = \{a \in A : \mathrm{Trd}(\sigma(a)b) \in R\}$ is the corresponding dual lattice, the **different** is the ideal $(\Lambda^\vee)^{-1} \subset \Lambda$ and the **discriminant** $\mathrm{Nrd}((\Lambda^\vee)^{-1}) \subset R$ is the ideal generated by the reduced norms of elements of the different.

Chapter VIII
Localization

VIII.1 Local algebras

We now recall some facts about division algebras over local fields. Let k be a local field, complete with respect to a discrete valuation v that is normalized such that $v(k^\times) = \mathbb{Z}$. Let $\mathfrak{o} := \{x \in k : v(x) \geq 0\}$ be the valuation ring and let $\mathfrak{p} := \pi\mathfrak{o} = \{x \in K : v(x) > 0\}$ be the valuation ideal, where $\pi \in k^\times$ is a prime element. Let D/k be a division algebra whose center contains k. There is a unique ([1] Theorem 12.10) extension of v to D that we also denote by v, defined on $a \in D$ as

$$v(a) := \frac{v(\mathrm{N}_{D/k}(a))}{\dim_k(D)} = \frac{v(\mathrm{N}_{k(a)/k}(a))}{\dim_k(k(a))}.$$

If $f \in k[x]$ is the minimal polynomial of $a \in D$, then $\dim_k(k(a)) = [k(a) : k] = \deg(f)$ and $\mathrm{N}_{k(a)/k}(a) = (-1)^{[k(a):k]} f(0)$. The valuation ring $\mathcal{O}_D = \{a \in D : v(a) \geq 0\}$ is the unique maximal order of D and is also the integral closure of $\mathfrak{o}$ in D. The valuation ideal is $\pi_D\mathcal{O}_D = \{a \in D : v(a) > 0\}$, where $\pi_D \in D^\times$ is a prime element. One can show ([1] Theorem 13.2) that $\overline{\mathcal{O}}_D := \mathcal{O}_D/\pi_D\mathcal{O}_D$ is a division algebra over the residue field $\mathbb{F} := \mathfrak{o}/\mathfrak{p}$. The **ramification index** $e(D/k)$ and **inertial degree** $f(D/k)$ of D/k are defined as

$$e(D/k) := [v(D^\times) : v(k^\times)] = \frac{1}{v(\pi_D)}, \quad f(D/K) := \dim_{\mathbb{F}}(\overline{\mathcal{O}}_D)$$

and satisfy $\dim_k(D) = e(D/k)f(D/k)$ ([1] Theorem 13.3). The value group is then $v(D^\times) = \frac{1}{e(D/k)}\mathbb{Z}$, and [1] defines a corresponding normalized valuation $v_D = e(D/k)v$ with value group $\mathbb{Z}$. If $\overline{\mathfrak{o}}$ is a finite field and $\dim_k(D) = n^2$, then $e(D/k) = f(D/k) = n$ ([1] Theorem 14.3).

Given a prime ideal $\mathfrak{p}$ of R, let $k_\mathfrak{p}$ be the corresponding completion and let $A_\mathfrak{p} = A \otimes_k k_\mathfrak{p}$. By the Artin-Wedderburn Theorem I.5.2, there is a central division algebra $D_\mathfrak{p}/k_\mathfrak{p}$, unique up to $k_\mathfrak{p}$-isomorphism, such that $A_\mathfrak{p} \simeq D_\mathfrak{p}^{\kappa_\mathfrak{p} \times \kappa_\mathfrak{p}}$. The corresponding normalized valuation $v_\mathfrak{p}$ satisfies $v_\mathfrak{p}(k) = \mathbb{Z}$ and admits a unique extension to $D_\mathfrak{p}$, satisfying $v_\mathfrak{p}(D_\mathfrak{p}) = \frac{1}{e_\mathfrak{p}}\mathbb{Z}$, where $e_\mathfrak{p} := e(D_\mathfrak{p}/k_\mathfrak{p})$. When k is a global field, then $e_\mathfrak{p}$ is equal to the **local index** $m_\mathfrak{p}$ of A at $\mathfrak{p}$, defined as the degree of the division algebra $D_\mathfrak{p}/k_\mathfrak{p}$ appearing in the isomorphism $A_\mathfrak{p} \simeq D^{\kappa_\mathfrak{p} \times \kappa_\mathfrak{p}}$ ([1] p. 222) calls $\kappa_\mathfrak{p}$ the **local capacity** of A at $\mathfrak{p}$). Note that $m_\mathfrak{p}$ is just the index of the localization $A_\mathfrak{p}$ in the usual sense.

VIII.2 Localizations of maximal orders

If R is an integral domain, the localization $S^{-1}\mathcal{O}$ of any R-order $\mathcal{O}$ with respect to a multiplicatively closed set $S \subset R$ is an $S^{-1}R$-order that is maximal if $\mathcal{O}$ is maximal [1].

If $S = R - \mathfrak{p}$ for a prime ideal $\mathfrak{p} \subset R$, then both $R_{\mathfrak{p}} := (R-\mathfrak{p})^{-1}R$ and $\mathcal{O}_{\mathfrak{p}} := \mathcal{O} \otimes_R R_{\mathfrak{p}} = (R-\mathfrak{p})^{-1}\mathcal{O}$ are local rings. So returning to our earlier setting, given a prime ideal $\mathfrak{p} \subset R$, we can recover the corresponding prime ideal $P \subset \mathcal{O}$ via $\mathfrak{p} \mapsto P = \mathcal{O} \cap \mathrm{rad}(\mathcal{O}_{\mathfrak{p}})$, and that $\mathrm{rad}(\mathcal{O}_{\mathfrak{p}}) = P\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}P$.

VIII.3 Approximation theorems

Weak approximation for $\mathbb{Q}$ ([4] Lemma 3.3.2):
Given $x_p \in \mathbb{Q}_p$ for every p in a finite set S of places and an $\epsilon > 0$, there exists an $x \in \mathbb{Q}$ such that $|x - x_p|_p < \epsilon$ for every $p \in S$. In other words, for any $m \in \mathbb{N}$, there exists an $x \in \mathbb{Q}$ such that $x \equiv x_p \bmod p^m$ for every $p \in S$.

This follows from the independence of valuations on $\mathbb{Q}$. In its most general form, the latter follows from the following statement (see Lang's *Algebra*): *Given finitely many inequivalent valuations ν on a field F, the diagonal embedding $F \to \prod_\nu F_\nu$ is dense.*
It is also a consequence of the following stronger version:

Strong approximation for $\mathbb{Z}$ ([4] Lemma 3.3.1): *Given $x_p \in \mathbb{Z}_p$ for every p in a finite set S of primes and an $\epsilon > 0$, there exists an $x \in \mathbb{Z}$ such that $|x - x_p|_p < \epsilon$ for every $p \in S$. Equivalently, this means that for any $m \in \mathbb{N}$, there exists an $x \in \mathbb{Z}$ such that $x \equiv x_p \bmod p^m$.*

The proof is basically just the **Chinese remainder theorem**:
Let $x_d \in \mathbb{Z}$ for d in a finite set of relatively prime positive integers d. Then there exists an $x \in \mathbb{Z}$ such that $x \equiv x_d \bmod d$ for each d.

The weak approximation theorem generalizes (at least) to rational orthogonal groups:

Weak approximation for orthogonal groups ([4] Theorem 9.7.2):
Let V be a nondegenerate rational quadratic space and let S be a finite set of places. Given $g_p \in \mathrm{SO}(V_{\mathbb{Q}_p})$ for every p in a finite set of places S, there exists a $g \in \mathrm{SO}(V)$ approximating the g_p arbitrarily well in the above sense.

Equivalently,

The image of $\mathrm{SO}(V)$ under the diagonal embedding $\mathrm{SO}(V) \to \prod_{p \in S} \mathrm{SO}(V_{\mathbb{Q}_p})$ is dense.

Under certain conditions, strong approximation also generalizes:

Strong approximation for indefinite spin groups ([4] Theorem 10.7.1):
Let Λ be a $\mathbb{Z}$-lattice of rank $n \geq 3$ equipped with an indefinite $\mathbb{Q}$-valued quadratic form and for each finite prime p, let $U_p \subset \mathrm{Spin}(\Lambda_{\mathbb{Q}_p})$ be an open set such that $U_p = \mathrm{Spin}(\Lambda_{\mathbb{Q}_p})$ away from a finite set S of finite primes. Then there exists a $g \in \mathrm{Spin}(\Lambda_{\mathbb{Q}})$ such that $g \in U_p$ for all finite primes p.

The utility of strong approximation in this context is that it implies a useful corollary for the spinor kernels in the following sense.

Corollary: *The same statement holds for the kernel Θ of the spinor norm on* SO.

This corollary fails for the entire orthogonal groups SO because, unlike Spin, they are not simply-connected as algebraic groups.

VIII.4 Grothendieck-Witt group

The **Witt group** $W(F)$ of a field F consists of isometry classes of anisotropic quadratic spaces over the field F, with operations

$$[V] + [V'] = [(V \oplus V')_a], \quad -[V] = [[-1]V].$$

Here, $[V]$ denotes the isometry class of the quadratic space V. Note that $[V]$ and $[-V]$ are additive inverses because $V \oplus -V \simeq H^{\oplus \dim(V)}$ and thus $(V \oplus -V)_a = 0$. There is a homomorphism $W(F) \to Q(F)$ taking the class of V to $(\mathrm{disc}(V), \dim(V) \bmod 2)$.

The Witt group is a quotient of the **Grothendieck-Witt group** $\widehat{W}(F)$. This is the Grothendieck group of the *Grothendieck-Witt semigroup* $\widehat{W}_0(F)$ whose elements are isomorphism classes $[V]$ of nondegenerate quadratic spaces V with addition defined as $[V]+[W] = [V \oplus W]$. These are the same relations as in the Witt group, except that $[-V]$ is no longer the additive inverse of $[V]$ because we are no longer disregarding hyperbolic spaces. Instead, $\widehat{W}(F)$ consists of formal differences $[V]-[W]$ of isomorphism classes of quadratic spaces. We can also define a multiplicative structure on these groups, giving the **Witt ring** and **Grothendieck-Witt ring** of F. It is possible to show that the additive subgroup $\langle [H_F] \rangle$ of $\widehat{W}(F)$ is also an ideal with respect to the ring structure on $\widehat{W}(F)$, giving an isomorphism of commutative rings

$$\widehat{W}(F)/\langle [H_F] \rangle \simeq W(F).$$

What are these rings for various choices of F? We have $W(\mathbb{R}) = \mathbb{Z}$ and $\widehat{W}(\mathbb{R}) = \mathbb{Z}/2$.

Howe says that $\mathbb{F}_q^\times / \mathbb{F}_q^{\times 2}$ generates $\widehat{W}(\mathbb{F}_q)$.

For $W(\mathbb{F}_p)$, with p an odd prime, there is different behavior depending on the value of $p \bmod 4$. If $p \equiv 1 \bmod 4$, we have $[1] = [-1]$, so that $[1] + [1] = [H_{\mathbb{F}_p}]$ in $\widehat{W}(K)$ and $[1] + [1] = 0$ in $W(F)$. The group $\widehat{W}(\mathbb{F}_p) = \langle [u_p] \rangle$, where u_p is any nonsquare in $\mathbb{F}_p^\times$ although we may take $\widehat{W}(\mathbb{F}_p) = \langle [-1] \rangle$ if $p \equiv 3 \bmod 4$.

VIII.5 Quadratic forms

Let M and S be modules over a ring R. A **quadratic form** $q\colon M \to S$ is a map such that $q(rv) = r^2 q(v)$ for every $r \in R$ and $v \in M$ and such that the map $B_q\colon M \times M \to S$ defined by

$$B_q(v,w) = q(v+w) - q(v) - q(w)$$

is R-bilinear. We call B_q the bilinear symmetric form **associated** to q. When $R = S$ is a field and M is a vector space V then (V,q) is called **quadratic space**. When $R = S = \mathbb{Z}$ and S is a free $\mathbb{Z}$-module Λ then (Λ, q) is called a **quadratic lattice**. When M is a torsion-free module Λ over $R = S$, then (Λ, q) is an **quadratic R-lattice**.

We will largely be concerned with **integral** lattices (Λ, q) for which one requires that q be **classically integral**, meaning that $q(x) = B(x,x)$ for some bilinear symmetric form $B\colon \Lambda \times \Lambda \to \mathbb{Z}$, necessarily satisfying $B_q = 2B$. A quadratic lattice (Λ, q) is **even** if $q(\Lambda) \subset 2\mathbb{Z}$ and otherwise it is **odd**. In particular,

$$\Lambda \text{ even } \Rightarrow \Lambda \text{ integral}, \quad \Lambda \text{ integral} \Rightarrow [2]\Lambda \text{ even},$$

where $[a]\Lambda = (\Lambda, aq)$ for a quadratic lattice (Λ, q). Given any symmetric integer matrix K, we have that $(\Lambda, K) := (\Lambda, K_{ij}x_ix_j)$ is an integral lattice that is even if each $K_{ii} \in 2\mathbb{Z}$ and is otherwise odd. When it is even, note that $(\Lambda, \frac{1}{2}K)$ is a quadratic lattice that is not classically integral.

Given a quadratic R-lattice (Λ, q), define the **dual** lattice

$$\Lambda^* = \mathrm{Hom}(\Lambda, R) \simeq \{y \in \Lambda_{\mathbb{Q}} : B_q(\Lambda, y) \subset R\}.$$

and the **classical dual** lattice

$$\Lambda^{\#} = \mathrm{Hom}(\Lambda, 2R) \simeq \{y \in \Lambda_{\mathbb{Q}} : B_q(\Lambda, y) \subset 2R\} = [2]\Lambda^*,$$

where we write $[a]\Lambda$ for the quadratic lattice (Λ, aq). If Λ is classically integral, then

$$\Lambda^* \simeq \{y \in \Lambda_{\mathbb{Q}} : 2B(\Lambda, y) \subset R\} \text{ and } \Lambda^{\#} \simeq \{y \in \Lambda_{\mathbb{Q}} : B(\Lambda, y) \subset R\},$$

in which case $\Lambda^{\#}$ coincides with the usual notion of dual lattice from the theory of integral lattices. We have $(\mathbb{Z}^n, K)^{\#} \simeq (\mathbb{Z}^n, K_{ij}^{-1})$ and $\Lambda^* \simeq (\mathbb{Z}^n, \frac{1}{2}K_{ij}^{-1})$. Note that $[\Lambda^{\#} : \Lambda^*] = 2^{\mathrm{rank}(\Lambda)}$ and in fact we have an extension

$$0 \to \Lambda^{\#}/\Lambda \to \Lambda^*/\Lambda \to (\mathbb{Z}/2)^n \to 0.$$

Probably this splits when $2 \nmid [\Lambda^{\#} : \Lambda]$.

Let (Λ, q) and (Λ', q') be quadratic lattices. For any ring R extending $\mathbb{Z}$, we write $\Lambda_R = \Lambda \otimes_{\mathbb{Z}} R$ and extend q to Λ_R in the obvious way. Given rings $R' \supset R \supset \mathbb{Z}$, an **isometry** $\varphi\colon \Lambda_R \to \Lambda'_{R'}$ is an R-linear map for which $q = q' \circ \varphi$. We write $\mathrm{Isom}(\Lambda_R, \Lambda'_{R'})$ for the set of isometries from Λ_R to $\Lambda'_{R'}$ and write $\Lambda_R \simeq \Lambda'_R$ to mean that Λ_R and Λ'_R are **isometric**, i.e. that each of $\mathrm{Isom}(\Lambda_R, \Lambda'_R)$ and $\mathrm{Isom}(\Lambda'_R, \Lambda_R)$ is non-empty.

Isometries of rational quadratic spaces obey a local-global principle:

Theorem VIII.5.1 (Hasse-Minkowski) Let V and V' be quadratic spaces over $\mathbb{Q}$. Then $V \simeq V'$ iff $V_{\mathbb{R}} \simeq V'_{\mathbb{R}}$ and $V_{\mathbb{Q}_p} \simeq V'_{\mathbb{Q}_p}$ for every prime number p.

Isometries of quadratic lattices, on the other hand, do not generally obey a local-global principle. Instead, quadratic lattices Λ and Λ' are said to be in the same **genus** if $\Lambda_{\mathbb{R}} \simeq \Lambda'_{\mathbb{R}}$ and $\Lambda_{\mathbb{Z}_p} \simeq \Lambda'_{\mathbb{Z}_p}$ for every prime p.

Given any R-lattice Λ in a vector space V, there is a bijection

$$\{R\text{-lattices} \subset V\} \to \mathrm{GL}(V)/\mathrm{GL}(\Lambda).$$

Given a quadratic form q on V, we may take a further quotient to obtain the space of abstract lattices appearing in V:

$$\left\{ \begin{array}{c} \text{isometry classes} \\ \text{of } R\text{-lattices} \subset V \end{array} \right\} \to \mathrm{O}(V)\backslash\mathrm{GL}(V)/\mathrm{GL}(\Lambda).$$

We note that this space of double cosets is also in bijection with the $\mathrm{GL}(\Lambda)$-equivalence classes of quadratic forms on V isometric to q but for now we will not use this viewpoint as it does not generalize nicely to spinor genera.

Recall that

$$\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n \subset \prod{}' \mathbb{Q}_p = \mathbb{A}_f$$

where the **restricted direct product** $\prod'$ carries the product topology (its open sets are unions of products of open subsets of the $\mathbb{Q}_p$ that all but finitely many terms are contained in $\mathbb{Z}_p$) For a quadratic lattice $\Lambda \subset V$, let $\widehat{\Lambda} := \Lambda_{\widehat{\mathbb{Z}}} \subset V_{\mathbb{A}_f}$. While we still get the same bijection

$$\{\text{lattices} \subset V\} \to \mathrm{GL}(V_{\mathbb{A}_f})/\mathrm{GL}(\widehat{\Lambda}) \leftrightarrow \mathrm{GL}(V)/\mathrm{GL}(\Lambda)$$

on isometry classes of lattices, the adeles enable us to capture more arithmetic information about the lattices in V:

$$\left\{ \begin{array}{c} \text{lattices} \subset V \text{ in} \\ \text{the genus of } \Lambda \end{array} \right\} \to \mathrm{O}(V_{\mathbb{A}_f})/\mathrm{O}(\widehat{\Lambda}).$$

$$\left\{ \begin{array}{c} \text{isometry classes} \\ \text{of lattices} \subset V \\ \text{in the genus of } \Lambda \end{array} \right\} \to \mathrm{O}(V_{\mathbb{A}_f})\backslash\mathrm{GL}(V_{\mathbb{A}_f})/\mathrm{GL}(\widehat{\Lambda}).$$

$$\mathrm{Genus}(\Lambda) = \mathrm{O}(V)\backslash\mathrm{O}(V_{\mathbb{A}_f})/\mathrm{O}(\widehat{\Lambda}).$$

For an oriented lattice (Λ, θ), where θ is one of the two possible $\mathbb{Z}$-bases of the top exterior power of $\wedge^n\Lambda$, one has the **proper genus**

$$\mathrm{Genus}^+(\Lambda) = \mathrm{SO}(V)\backslash\mathrm{SO}(V_{\mathbb{A}_f})/\mathrm{SO}(\widehat{\Lambda}).$$

Example VIII.5.1 If $(\Lambda, q) = (\mathbb{Z}, x^2)$, then $B(x,y) = x.y$ and $B_q(x,y) = 2\,x.y$, giving $\Lambda^\# = \mathbb{Z}$ and $\Lambda^* = \frac{1}{2}\mathbb{Z}$. In particular, $\Lambda^*/\Lambda \simeq \mathbb{Z}/2$.

Example VIII.5.2 The lattice $(\mathbb{Z}^2, x_1x_2) = (\mathbb{Z}^2, \frac{1}{2}\sigma_x)$ is integral but not classically integral, whereas $(\mathbb{Z}^2, 2x_1x_2) = (\mathbb{Z}^2, \sigma_x)$ and $(\mathbb{Z}^2, x_1^2 - x_2^2) = (\mathbb{Z}^2, \sigma_z)$ are classically integral.

Example VIII.5.3 Let A/K be an algebra over a field K. Left multiplication by $a \in A$ is a K-linear transformation $\ell_a \colon A \to A$. The **relative norm** is the homomorphism $\mathrm{N}_{A/K} \colon A \to K$ defined by $\mathrm{N}_{A/K}(a) = \det(\ell_a)$ and the **relative trace** $\mathrm{Tr}_{A/K} \colon A \to K$ is the linear map $\mathrm{Tr}_{A/K}(a) = \mathrm{Tr}(\ell_a)$.

Example VIII.5.4 For a Galois extension F/K of number fields, the relative norm $\mathrm{N}_{F/K} \colon F \to K$ has the explicit formula

$$\mathrm{N}_{F/K}(x) = \prod_{\sigma \in \mathrm{Gal}(F/K)} x^\sigma.$$

Example VIII.5.5 A quadratic field $Q(\sqrt{D})$ has $\mathrm{N}_{Q(\sqrt{D})/\mathbb{Q}}(x + y\sqrt{D}) = x^2 - Dy^2$.

Example VIII.5.6 Let let A/K be a central simple algebra over a field K with $\dim_K A = n^2$ (the **degree** $[A : K]$ is $\sqrt{\dim_K A} = n$). Suppose that L is a splitting field for A, so that $A_L \simeq L^{n\times n}$. Therefore A contains a commutative subalgebra isomorphic to L and the K-algebra homomorphism $A \to L^{n\times n}$ given by composing the map $a \mapsto a \otimes 1_L$ with any isomorphism $A \otimes 1_L \to L^{n\times n}$ is injective. The **reduced norm** $\mathrm{Nrd} \colon A \to K$ is the quadratic form $\mathrm{Nrd}(a) = \det(a \otimes_K 1_L)$, which is also well-defined by replacing L with any number field splitting A. The **reduced trace** $\mathrm{Trd} \colon A \to K$ is similarly defined as $\mathrm{Trd}(a) = \mathrm{Tr}(a \otimes 1_L)$. These are related to the ordinary norm and trace (where we view A as a subalgebra of the superoperators $\mathrm{End}(L^{n\times n})$) via $\mathrm{Tr}(a) = n\,\mathrm{Trd}(a)$ and $\mathrm{N}(a) = \mathrm{Nrd}(a)^n$.

Example VIII.5.7 For a special case of the above, recall that a rational quaternion algebra $A = \left(\frac{a,b}{K}\right)$ over a field K carries a nontrivial involution taking $v = v_0 + v_1 i + v_2 j + v_3 ij$ to $\bar{v} = v_0 - v_1 i - v_2 j - v_3 ij$. Then

$$\mathrm{Nrd}(v) = v\bar{v} = v_0^2 - av_1^2 - bv_2^2 + abv_3^2 \ (= v_0^2 + v_1^2 + v_2^2 + v_2^2 \text{ if } a = b = -1)$$

and $\mathrm{Trd}(v) = v + \bar{v} = 2v_0$, with associated bilinear form

$$\begin{aligned} B_{\mathrm{Nrd}}(v,w) &= \mathrm{Nrd}(v+w) - \mathrm{Nrd}(v) - \mathrm{Nrd}(w) \\ &= \mathrm{Trd}(v\bar{w}) = v\bar{w} + w\bar{v} \\ &= 2(v_0w_0 - av_1w_1 - bv_2w_2 + abv_3w_3). \end{aligned}$$

On the other hand, we have another (untwisted) quadratic form

$$Q(v) = v^2 = v_0^2 + av_1^2 + bv_2^2 - abv_3^2 \ (= v_0^2 - v_1^2 - v_2^2 - v_3^2 \text{ if } a = b = -1)$$

along with its associated bilinear form $B_Q(v,w) = \mathrm{Trd}(vw)$.

VIII.5.1 Classifying quadratic lattices

Assume that $\Lambda_{\mathbb{R}} \simeq \Lambda'_{\mathbb{R}}$ (i.e. they have the same signature) and $\det(\Lambda) = \det(\Lambda')$. Then

$$\begin{array}{ccc}
\Lambda_{\mathbb{Q}} \simeq \Lambda'_{\mathbb{Q}} & \Longleftrightarrow & \Lambda_{\mathbb{Q}_p} \simeq \Lambda'_{\mathbb{Q}_p} \forall p \\
\Uparrow & & \Uparrow \\
\mathrm{Genus}(\Lambda) = \mathrm{Genus}(\Lambda') & \Longleftrightarrow & \Lambda_{\mathbb{Z}_p} \simeq \Lambda'_{\mathbb{Z}_p} \forall p \\
\Uparrow & & \Uparrow \\
\mathrm{SpGenus}(\Lambda) = \mathrm{SpGenus}(\Lambda') & \Longleftrightarrow & \begin{array}{c} \exists \Lambda'' \simeq_{\mathbb{Q}} \Lambda \\ \text{and } g_p \in \mathrm{Spin}(\Lambda_{\mathbb{Q}_p}) \\ \text{s.t. } g_p(\Lambda_{\mathbb{Z}_p}) = \Lambda''_{\mathbb{Z}_p}) \forall p. \end{array}
\end{array}$$

test

VIII.6 Global structure of algebras

Here are some fundamental structure theorems about algebras over global fields.

Hasse Norm Theorem. *Let F/K be cyclic and let $a \in K^\times$. Then $a \in \mathrm{N}_{F/K}(F^\times)$ iff, for every prime $\mathfrak{p}$ of K, $a \in \mathrm{N}_{F_\mathfrak{P}/K_\mathfrak{p}}(F_\mathfrak{P}^\times)$ for some (and hence any) prime $\mathfrak{P}$ of F dividing $\mathfrak{p}$.*

Some people (e.g. [8]) call it the Hilbert-Furtwängler-Hasse norm theorem as it was proved by Hilbert in 1897 for quadratic extensions, by Furtwängler in 1902 for extensions of prime degree, and by Hasse in 1931 for the general cyclic case.

Local global principle for algebras (Albert-Brauer-Hasse-Noether). *A central simple algebra A/K splits if and only if $A_{K_\mathfrak{p}}$ splits for every prime $\mathfrak{p}$ of K. Equivalently, the natural homomorphism*

$$\mathrm{Br}(K) \to \bigoplus_{\mathfrak{p}} \mathrm{Br}(K_\mathfrak{p})$$

is injective.

The image of $\mathrm{Br}(K)$ is precisely characterized via the following exact sequence

$$1 \to \mathrm{Br}(K) \to \bigoplus_{\mathfrak{p}} \mathrm{Br}(K_\mathfrak{p}) \xrightarrow{\sum \mathrm{inv}_\mathfrak{p}} \mathbb{Q}/\mathbb{Z} \to 0.$$

Main Theorem (Albert-Brauer-Hasse-Noether). *Every central simple algebra over a number field is cyclic.*
([8] p. 5, [1] p. 259). The proof follows from the next two theorems.

Given a Galois extension F/K of number fields and a prime $\mathfrak{p}$ of K, let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$. Then there a K-algebra isomorphism

$$F \otimes_K K_\mathfrak{p} \simeq \prod_{\mathfrak{P}|\mathfrak{p}} F_\mathfrak{P},$$

where the sum is over primes $\mathfrak{P}$ of F above $\mathfrak{p}$. All the $F_\mathfrak{P}$ are isomorphic because $\mathrm{Gal}(F/K)$ is Galois.

Given a field K, let $s(K)$ be the largest integer s for which $\mathbb{Q}(\zeta_{2^s} + \zeta_{2^s}^{-1}) \subset K$ but $\mathbb{Q}(\zeta_{2^s}) \not\subset K$. Then [27] K is called $s(K)$**-special**.

Grunwald-Wang Theorem. *Let K be a number field, let S_0 be the set of (necessarily even) primes $\mathfrak{p}$ for which $s(K) = s(K_\mathfrak{p})$. Given any finite set S of primes and any $n \in \mathbb{N}$, the group $(K^\times)^n$ of nth powers is equal to the subgroup*

$$K^\times \cap \bigcap_{\mathfrak{p} \in S} (K_\mathfrak{p}^\times)^n$$

of $K^\times$ containing those elements with an nth root in $K_\mathfrak{p}$ for each $\mathfrak{p} \in S$, unless $S_0 \subset S$ and $\mathrm{ord}_2(n) > s(K)$, in which case $(K^\times)^n$ is an index-2 subgroup. Wikipedia seems to rephrase [27] via the following three conditions: (i) $2^{s+1} \mid n$, (ii) K is s-special, (iii) every prime $\mathfrak{p}$ such that $K_\mathfrak{p}$ is s-special (such $\mathfrak{p}$ necessarily divide 2) is contained in S.

Roquette gives a slightly different formulation: For each $\mathfrak{p} \in S$, we are given a cyclic extension $L(\mathfrak{p})/K_{\mathfrak{p}}$. If n is divisible by all their degrees, then there exists a degree-n cyclic extension L/K such that $L_{\mathfrak{P}} \simeq L(\mathfrak{p})$ for every $\mathfrak{p} \in S$, where $\mathfrak{P}$ is any prime of L dividing $\mathfrak{p}$.

Chapter IX
Class numbers

Main source is [1] (ch. 15–16 on Morita equivalence, ch. 26 on ideal classes, ch. 27 on genus, ch. 36 on K_0 of maximal orders and ch. 37 on Picard groups). Other possible sources include Milnor's Introduction to algebraic K-theory, Lam's First Course on Noncommutative Rings.

IX.1 Morita equivalence

Two R-algebras A_1, A_2 are **Morita equivalent** if their categories A_1-mod and A_2-mod of modules are R-linearly equivalent. An A_1-A_2-bimodule M_{12} is R-**invertible** if there exists a **Morita context**, i.e. an A_2-A_1-bimodule M_{21} over R (on which the left and right R-actions coincide) together with bimodule isomorphisms

$$M_{12} \otimes_{A_2} M_{21} \simeq A_1, \;\; M_{21} \otimes_{A_1} M_{12} \simeq A_2$$

such that the following diagrams commute:

$$\begin{array}{ccc} M_{12} \otimes_{A_2} M_{21} \otimes_{A_1} M_{12} & \longrightarrow & A_1 \otimes_{A_1} M_{12} \\ \downarrow & & \downarrow \\ M_{12} \otimes_{A_2} A_2 & \longrightarrow & M_{12}, \end{array} \qquad \begin{array}{ccc} M_{21} \otimes_{A_1} M_{12} \otimes_{A_2} M_{21} & \longrightarrow & A_2 \otimes_{A_2} M_{21} \\ \downarrow & & \downarrow \\ M_{21} \otimes_{A_1} A_1 & \longrightarrow & M_{21}. \end{array}$$

Theorem IX.1.1 Two R-algebras A_1, A_2 are Morita equivalent iff there exists an invertible A_1-A_2-bimodule over R.

The group [1] (37.5) $\mathrm{Pic}_R(A)$ of isomorphism classes of invertible A-bimodules over R with multiplication $[M]\cdot[N] = [M \otimes_\Lambda N]$ is the (relative) Picard group. It is a subgroup of the absolute Picard group $\mathrm{Pic}(A) = \mathrm{Pic}_{\mathbb{Z}}(A)$, which accounts for all isomorphicm classes over $\mathbb{Z}$ and depends only on the underlying ring of A. Morita-equivalent rings have isomorphic centers and isomorphic Picard groups. Equivalence over R means their centers are R-linearly isomorphic.

IX.2 Two-sided ideal class group of an order

Let R be an integral domain with quotient field K and let $\mathcal{O}$ be an R-order in a K-algebra A. The group $I(\mathcal{O})$ of invertible two-sided $\mathcal{O}$-ideals in A lies in an exact sequence ([1] Theorem 37.23):

$$1 \to Z(\mathcal{O})^\times \to Z(A)^\times \to I(\mathcal{O}) \to \mathrm{Picent}(\mathcal{O}) \to \mathrm{Picent}(A).$$

If A is semisimple, then Corollary 37.24 of [1] shows that

$$\mathrm{Picent}(\mathcal{O}) \simeq I(\mathcal{O})/\{\mathcal{O}x : x \in (KZ(\mathcal{O}))^\times\}.$$

If A/K is furthermore central simple, then

$$\mathrm{Picent}(\mathcal{O}) = \mathrm{Pic}_R(\mathcal{O}) \simeq I(\mathcal{O})/P(\mathcal{O}),$$

where $P(\mathcal{O}) = \{\mathcal{O}x : x \in K^\times\}$ is the principal invertible two-sided $\mathcal{O}$-ideals in A.

IX.3 Genus and equivalence of fractional ideals

Throughout this section let R be a Dedekind domain with quotient field K and let $\mathcal{O}$ be an R-order in a K-algebra A.

Two left $\mathcal{O}$-ideals $M, N \subset A$ are isomorphic iff there exists an $a \in A^\times$ such that $Ma = N$. The **class number** $h(\mathcal{O})$ of $\mathcal{O}$ is the number of isomorphism classes of left $\mathcal{O}$-ideals in A under this right action. If A is semisimple and K is a global field, then $h(\mathcal{O})$ is finite by the the Jordan-Zassenhaus Theorem (Theorem 26.4 in [1]), which in this case states that there are finitely many isomorphism classes of left $\mathcal{O}$-lattices of a given finite rank.

Two left $\mathcal{O}$-lattices M, N are in the same **genus** if $N_\mathfrak{p} \simeq M_\mathfrak{p}$ as $\mathcal{O}_\mathfrak{p}$-ideals for every prime ideal $\mathfrak{p} \subset R$. If $\mathcal{O}$ is maximal and K is separable, then ([1] Theorem 27.4) all left $\mathcal{O}$-ideals of A are in the same genus as $\mathcal{O}$, and if $M_1, \ldots, M_n$ are left $\mathcal{O}$-ideals in A, there exists a left $\mathcal{O}$-ideal M such that

$$M_1 \oplus \cdots \oplus M_n \simeq \mathcal{O}^{\oplus n-1} \oplus M.$$

If A is a central simple K-algebra, the genus considerations above imply ([1] 35.5) that the stable isomorphism classes of left $\mathcal{O}$-ideals of A form an abelian group that, when $\mathcal{O} = R$, coincides with the ordinary class group of isomorphism classes of fractional R-ideals of K, with $\mathfrak{a}, \mathfrak{b} \subset K$ isomorphic precisely when they are isomorphic as R-modules, or equivalently, when $\mathfrak{a} = \mathfrak{b}x$ for some $x \in K$.

When A is furthermore separable, the group of two-sided $\mathcal{O}$-ideals can be described as follows. Theorem 37.28 of [1] shows that if A is separable, there is an exact sequence

$$1 \to \mathrm{Picent}(Z(\mathcal{O})) \to \mathrm{Picent}(\mathcal{O}) \to \prod_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathrm{Picent}(\mathcal{O}_\mathfrak{p}) \to 1$$

where $\mathcal{O}_\mathfrak{p}$ denotes $\mathfrak{p}$-adic completion. Corollary 37.32 of [1] then shows that when $\mathcal{O}$ is a maximal R-order and A is a central-simple K-algebra, then

$$1 \to \mathrm{CL}(R) \to \mathrm{Picent}(\mathcal{O}) \to \prod_\mathfrak{p} \mathbb{Z}/e_\mathfrak{p} \to 1,$$

where the $e_\mathfrak{p}$ is the ramification index of the division algebra $D = \mathrm{Hom}_{K_\mathfrak{p}}(A_\mathfrak{p})$ in the Brauer class of $A_\mathfrak{p}$, which is 1 except possibly for primes $\mathfrak{p}$ dividing $\mathrm{disc}(\mathcal{O})$. Over global fields, $e_\mathfrak{p}$ is the local index $m_\mathfrak{p}$ of A at $\mathfrak{p}$.

IX.4 Class groups and K_0

Let R be a commutative ring. If P is a projective R-module, let $[P]$ be its isomorphism class. The Grothendieck ring of the category of finite generated projective R-modules is

$$K_0(R) = \Big\langle [P] : P \Big\rangle \Big/ \Big\langle [P] + [Q] - [P \oplus Q] : P, Q \Big\rangle.$$

Elements of $K_0(R)$ correspond to stable isomorphism classes of projective R-modules because $[P] = [Q]$ iff $P \oplus R^n \simeq Q \oplus R^n$ for some n. I think that

$$K_0(R) = \{\text{rank-1 projective } R\text{-modules}\}/\{\text{rank-1 free } R\text{-modules}\}$$

but I'm not sure if this requires further qualifications of R. A multiplication is defined on $K_0(R)$ via $[P] \cdot [Q] = [P \otimes_R Q]$, making $K_0(R)$ into a commutative ring whose unit group $K_0(R)^\times$ is equal to the the **Picard group**

$$\mathrm{Pic}(R) = \{\text{invertible fractional ideals of } R\}/\{\text{principal fractional ideals of } R\}.$$

and the **ideal class monoid** of an integral domain R is

$$\mathrm{CL}(R) = \{\text{fractional ideals of } R\}/\{\text{principal fractional ideals of } R\}.$$

These sit in an exact sequence

$$1 \to R^\times \to K^\times \to \{\text{invertible fractional } R\text{-ideals}\} \to \mathrm{Pic}(R) \to 1.$$

In general $\mathrm{Pic}(R)$ is defined to be the group of invertible sheaves on $\mathrm{Spec}(R)$. When R is a Dedekind domain, R is a smooth affine curve. The Noetherian domain $\mathbb{Z}[\sqrt{5}]$ satisfies $\mathrm{Spec}(\mathbb{Z}[\sqrt{5}]) = \mathrm{Spec}\Big(\mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big]\Big) \setminus (2)$. In general if $\mathcal{O} \subset K$ is an order the ring class group is $\mathrm{Pic}(\mathcal{O}) \simeq \mathrm{Gal}(K^{\mathcal{O}}/K^{(1)})$.

IX.5 Morita equivalence for local rings

If A is a local ring, its Morita equivalence class consists of the rings $A^{n\times n}$ of matrices over A.

Note below that division algebras are local, which implies the corresponding structure for CSAs.

Chapter X
Appendix

X.1 Modular categories

A **modular category** is a premodular category for which S is invertible. Together with the T-matrix $T = \mathrm{diag}(\{\theta_a\})$ this defines a projective unitary representation of $\mathrm{SL}_2(\mathbb{Z})$ mapping $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \mapsto [S]$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \mapsto [T]$.

X.2 Super and spin modular categories

If C is a braided fusion category, its **Muger center** $\mathsf{Z}_2(\mathsf{C}) = \mathsf{C}'$ (a.k.a. *symmetric center*) is the (symmetric) fusion subcategory generated by the simple objects that braid trivially with everything else. A premodular category C is modular iff $\mathsf{C}' = \mathsf{Vec}$ and is called **super modular** if $\mathsf{C}' = \mathsf{sVec} = \mathsf{Rep}(\mathbb{Z}/2, -1)$. It is symmetric iff $\mathsf{C}' = \mathsf{C}$.

A super modular category satisfies

$$S = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \hat{S}, \;\; T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \hat{T},$$

where $\hat{S}$ is unique but $\hat{T}$ only unique up to a sign (cf quadratic refinement). See [28]: $\langle \hat{S}, \hat{T} \rangle$ finite when C has a minimal modular extension..

If C is a fusion category, then the **Drinfeld center** $\mathsf{Z}_1(\mathsf{C})$ is a modular category.

Spin modular category is a modular category with a distinguished fermion (i.e. a simple object f with $f \otimes f \simeq 1$). A modular extension of a super modular category is spin modular.

X.3 2+1D TQFTs with boundary

(Super)modular categories classify (spin)TQFTs. The objects of the category are local excitations in the TQFT. The gauss sums $p^{\pm}$ of the modular category of a TQFT on $D^2 \times \mathbb{R}$ and the central charge c_- of a CFT on the boundary $S^1 \times \mathbb{R}$ must satisfy

$$e^{2\pi i c_-/8} = p_+/\mathcal{D} = \sqrt{p_+/p_-}.$$

$$\{\text{cats}\} \xrightarrow{\mathsf{Z}_0} \{\otimes\text{-cats}\} \xrightarrow{\mathsf{Z}_1} \{\text{braided} \otimes\text{-cats}\} \xrightarrow{\mathsf{Z}_2} \{\text{symmetric} \otimes\text{-cats}\}$$

Monoidal center $\mathsf{Z}_0(\mathsf{C}) = \mathrm{End}(\mathsf{C})$

Drinfeld center $\mathsf{Z}_1(\mathsf{T}) =$ quantum double

Symmetric (Muger) center $\mathsf{Z}_2(\mathsf{B}) = \{a : c_{a,b} = 1 \ \forall b \in \mathsf{B}\}$

X.4 Association schemes

Let X be a set. An **association scheme** on X with m classes is a set of subsets $R_0, R_1, \ldots, R_m \subset X \times X$ satisfying

1. $\biguplus_{a=0}^{n} R_a = X \times X$
2. $R_0 = \{(x, x) : x \in X\}$
3. For each a, there is an a' such that $R_{a'} = \{(y, x) : (x, y) \in R_a\}$.
4. There exist $N_{ab}^c \in \mathbb{N}_0$ such that for all $(a, b) \in R_c$,

$$N_{ab}^c = |\{z : (x, z) \in R_a \text{ and } (z, y) \in R_b\}|.$$

Given an association scheme, let $A_i \in \{0, 1\}^{|X|\times|X|}$ be such that $(A_i)_{xy} = 1$ only when $(x, y) \in R_i$. Then

1. $\sum_i A_i$ is the all-1 matrix.
2. $A_0 = I$
3. For each i, there is an i' such that $A_i^T = A_{i'}$
4. $\mathbb{Z}[A_0, A_1, \ldots, A_m] = \mathbb{Z}A_0 + \mathbb{Z}A_1 + \cdots + \mathbb{Z}A_m$, i.e. $A_i A_j = \sum_k N_{ij}^k A_k$ for some $N_{ij}^k \in \mathbb{N}_0$.

This serves as an alternative definition of an association scheme.

X.5 Triangulated categories

A **translation** or **shift** functor on a category C is an additive automorphism $\Sigma : \mathsf{C} \to \mathsf{C}$. Write $a[n] = \Sigma^n a$ for the degree shift. A **triangulated category** is an additive category C with a shift functor equipped with a family of **exact triangles**

$$a \to b \to c \to a[1]$$

satisfying a bunch of conditions.

Examples include the derived category of any abelian category and the stable homotopy category. Different abelian categories can have equivalent derived categories, and **t-structures** parameterize these different degree-0 abelian subcategories.

There is also a K_0 for a triangulated category. The homotopy category of a stable ∞-category has a canonical triangulation, whose K_0 is generalized by the higher K_is of the stable ∞-category.

X.6 Grothendieck topologies

`https://en.wikipedia.org/wiki/Grothendieck_topology`

A **subfunctor** $\mathcal{G} \subset \mathcal{F}$ of a presheaf $\mathcal{F}$ is presheaf $\mathcal{G}$ such that $\mathcal{G}(U) \subset \mathcal{F}(U)$ for all objects U and $\mathcal{G}(f) = \mathcal{F}(f)|_{\mathcal{G}(x)}$ for all morphisms $f : V \to U$.

A **sieve** on an object $U \in \mathsf{C}$ is a subfunctor $\mathcal{S}(U)$ of the functor of points $\mathrm{Hom}(-, U)$. For each morphism $f : V \to U$, the **pullback**

$$f^*\mathcal{S}(U) = \mathcal{S}(U) \times_{\mathrm{Hom}(-,U)} \mathrm{Hom}(-, V) \hookrightarrow \mathrm{Hom}(-, V)$$

is a sieve on V. A **Grothendieck topology** J on C consists of **covering sieves** $J(U)$ on the objects U satisfying the following conditions:

- If $f : V \to U$, then $f^* : J(U) \to J(V)$.
- $\mathrm{Hom}(-, U) \in J(U)$ for all $U \in \mathsf{C}$.
- If $\mathcal{S} \in J(U)$ and a sieve $\mathcal{T}$ on U satisfies $f^*\mathcal{T} \in J(V)$ for all $f \in \mathcal{S}(U) \cap \mathrm{Hom}(V, U)$, then $\mathcal{T} \in J(U)$.

A Grothendieck topology can also be specified in terms of a **Grothendieck pretopology** consisting of **covering families** (see above Wikipedia page for now) if C has enough fibered products.

A **site** is a category equipped with a Grothendieck topology. Each topological space determines a site and the space can be recovered iff it is **sober**. Luckily the Zariski topology is sober. Sober sits in-between T_1 and T_2. See

`https://en.wikipedia.org/wiki/Sober_space`

A **sheaf** on a site (C, J) is a presheaf $\mathcal{F}$ on C such that

$$\mathrm{Hom}(\mathrm{Hom}(-, U), \mathcal{F}) \to \mathrm{Hom}(\mathcal{F}, U)$$

is a bijection for all U.

X.7 Quivers

A **quiver** $\Gamma = (V, E)$ is a directed multigraph with possible self-loops. A **representation** of Γ is a functor from its category $\mathsf{Path}(\Gamma)$ of paths to another linear category such as the category of finite-dimensional vector spaces over some field.

A quiver is of **finite type** if it has finitely many isomorphism classes of indecomposable representations.

Theorem X.7.1 (Gabriel's Theorem [29]) The finite-type connected quivers are the ADE diagrams and their indecomposable representations correspond to the the positive roots of the corresponding root systems.

X.8 Stacks

`https://stacks.math.columbia.edu/tag/0268`

Bibliography

[1] I. Reiner, *Maximal Orders*. Clarendon Press, 1975, 395 pp.

[2] M.-A. Knus, A. Merkurjev, M. Rost, and P. Tignol, *The Book of Involutions*, ser. Colloquium Publications / American Mathematical Society v. 44. Providence, R.I: American Mathematical Society, 1998, 593 pp.

[3] T.-Y. Lam, *A First Course in Noncommutative Rings*. Springer Science & Business Media, Jun. 21, 2001, 416 pp.

[4] J. W. S. Cassels, *Rational Quadratic Forms*. Courier Dover Publications, Aug. 8, 2008, 429 pp.

[5] M.-A. Knus, *Quadratic and Hermitian Forms over Rings*, red. by M. Artin, S. S. Chern, J. Coates, *et al.*, ser. Grundlehren Der Mathematischen Wissenschaften. Berlin, Heidelberg: Springer, 1991, vol. 294.

[6] W. Scharlau, *Quadratic and Hermitian Forms*, red. by M. Artin, S. S. Chern, J. M. Fröhlich, *et al.*, ser. Grundlehren Der Mathematischen Wissenschaften. Berlin, Heidelberg: Springer, 1985, vol. 270.

[7] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, 1st ed. Cambridge University Press, Aug. 10, 2006.

[8] P. Roquette, *The Brauer-Hasse-Noether Theorem in Historical Perspective*. Springer Science & Business Media, Mar. 30, 2006, 92 pp.

[9] J. C. McConnell and J. C. Robson, *Noncommutative Noetherian Rings*. American Mathematical Soc., 2001, 658 pp.

[10] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*. Springer Science & Business Media, Feb. 9, 2006, 474 pp.

[11] P. Etingof, S. Gelaki, D. Nikshych, and V. Ostrik, *Tensor Categories*, ser. Mathematical Surveys and Monographs. Providence, Rhode Island: American Mathematical Society, 2015, vol. 205, 343 pp.

[12] A. Blass, "Injectivity, projectivity, and the axiom of choice," *Transactions of the American Mathematical Society*, vol. 255, pp. 31–59, 1979. JSTOR: 1998165.

[13] E. Bannai, "Association schemes and fusion algebras (an introduction)," *Journal of Algebraic Combinatorics*, vol. 2, no. 4, pp. 327–344, Nov. 1, 1993.

[14] A. A. Albert, *Structure of Algebras*. American Mathematical Society, 1939, 210 pp.

[15] R. Vakil, "The Rising Sea - Foundations of Algebraic Geometry."

[16] R. Hartshorne, *Algebraic Geometry*. Springer Science & Business Media, Dec. 19, 1977, 520 pp.

[17] C. DeConcini, D. Eisenbud, and C. Procesi, "Young diagrams and determinantal varieties," *Inventiones mathematicae*, vol. 56, no. 2, pp. 129–165, Feb. 1, 1980.

[18] D. Murfet, *Graded rings and modules*, therisingsea.org, 2006.

[19] A. Bak, *K-Theory of Forms. (AM-98)*. Princeton University Press, 1981. JSTOR: j.ctt1b9s087.

[20] S. Lang, *Algebra*, 3rd edition. New York: Springer/Sci-Tech/Trade, Apr. 2, 2002, 918 pp.

[21] C. T. C. Wall, "Graded algebras, anti-involutions, simple groups and symmetric spaces," *Bulletin of the American Mathematical Society*, vol. 74, no. 1, pp. 198–202, Jan. 1968.

[22] T.-Y. Lam, *Introduction to Quadratic Forms over Fields*. American Mathematical Soc., 2005, 577 pp.

[23] C. T. C. Wall, "Graded Brauer Groups," *Journal fr die reine und angewandte Mathematik*, vol. 1964, no. 213, pp. 187–199, Jan. 1, 1964.

[24] J. Helmstetter and A. Micali, *Quadratic Mappings and Clifford Algebras*. Basel Boston: Birkhäuser, 2008.

[25] P. Lounesto, *Clifford Algebras and Spinors*. Cambridge University Press, May 3, 2001, 352 pp.

[26] C. Chevalley, *The Algebraic Theory of Spinors and Clifford Algebras: Collected Works*. Springer Science & Business Media, Dec. 13, 1996, 232 pp.

[27] E. Artin and J. T. Tate, *Class Field Theory*. Providence, R.I: AMS Chelsea Pub, 2009, 192 pp.

[28] P. Bonderson, E. C. Rowell, Q. Zhang, and Z. Wang, "Congruence Subgroups and Super-Modular Categories," *Pacific Journal of Mathematics*, vol. 296, no. 2, pp. 257–270, Jul. 16, 2018. arXiv: 1704.02041 [math].

[29] P. Gabriel, "Unzerlegbare Darstellungen I," *manuscripta mathematica*, vol. 6, no. 1, pp. 71–103, Mar. 1, 1972.