Part I
Introduction

One of the first questions one asks of a problem in Mathematics is whether there exists a solution. Oftentimes there is no guarentee that a solution exists, however we can use this failure of existence to construct something positive. Cohomology is a tool which is used for this purpose. In this set of notes, we will describe one example of a cohomology theory: Galois Cohomology. Before we describe the general theory, we want to give a motivating example.

Example 0.1. Consider the following matrices M, $M_0 \in \mathrm{M}_2(\mathbb{Z})$

$$M_0 = \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix} \qquad M = \begin{pmatrix} 0 & 5 \\ -1 & 0 \end{pmatrix}$$

It's easy to see that M_0 is the matrix representation for $\sqrt{-5}$ on the $\mathbb{Z}$-basis $\{1, \sqrt{-5}\}$ and M is the matrix representation for $\sqrt{-5}$ on the $\mathbb{Z}$-basis $\{1, -\sqrt{-5}\}$. Even though these two matrices are $\mathrm{GL}_2(\mathbb{Z})$-conjugate, they are not $\mathrm{SL}_2(\mathbb{Z})$-conjugate. Indeed, they are not even $\mathrm{SL}_2(\mathbb{Q})$-conjugate, but it turns out that they are $SL_2(\mathbb{Q}(i))$-conjugate. A change of basis matrix from $\{1, \sqrt{-5}\}$ to $\{1, \sqrt{-5}\}$ is given by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Of course, this matrix has determinant -1, so it is not in $SL_2(\mathbb{Q}(i))$, but if we multiply this matrix by i, then we get a matrix which is in $SL_2(\mathbb{Q}(i))$. So we have a problem which has no solution in $\mathbb{Q}$, but does have a solution in $\mathbb{Q}(i)$.

Let's describe how to constuct something positive out of this non-solution using Galois cohomology. Let $G = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ and define $Z_{SL_2}(M_0)(\mathbb{Q}(i))$ to be the set of all $Q \in SL_2(\mathbb{Q}(i))$, such that Q commutes with M_0, and define $SL_2(\mathbb{Q}(i)) \star M_0$ to be the set of all matrices of the form QM_0Q^{-1}. Observe that we have the following short exact sequence of pointed G-sets:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Z_{SL_2}(M_0)(\mathbb{Q}(i)) & \longrightarrow & SL_2(\mathbb{Q}(i)) & \longrightarrow & SL_2(\mathbb{Q}(i)) \star M_0 & \longrightarrow & 0 \\ & & & & Q & \longmapsto & QM_0Q^{-1} & & \end{array}$$

Now apply the following galois cohomology functor which maps a G-set X to the G-set X^G, i.e. the set of all $x \in X$ such that $g \cdot x = x$, to the short exact sequence above. Since this is a left-exact functor we get a long exact sequence of the form

$$0 \longrightarrow Z_{SL_2}(M_0)(\mathbb{Q}) \longrightarrow SL_2(\mathbb{Q}) \longrightarrow SL_2(\mathbb{Q}) \star M_0 \xrightarrow{\ \delta\ } H^1(G, Z_{SL_2}(M_0)(\mathbb{Q})) \longrightarrow H^1(G, SL_2(\mathbb{Q})) \longrightarrow \cdots$$

What happened here is that we have lost surjectivity after applying the functor: the matrix M is not in the image of anything from $SL_2(\mathbb{Q})$. Galois cohomology measures the failure of this surjectivity, by constructing a map δ. The way the δ map works is it takes this matrix M and constructs a function from G to $Z_{SL_2}(M_0)(\mathbb{Q})$ as follows: We go back to the short exact sequence before the functor was applied. Then we lift $M \in SL_2(\mathbb{Q}(i))\star$

Let k^{sep} be a seperable closure of a field k, and denote G_k to mean $Gal(k^{sep}/k)$. Let $n \geq 1$ be an integer, and assume that the image of n in k is nonzero. Then associated to the exaxt sequence

$$0 \longrightarrow \mu_n \longrightarrow (k^{sep})^* \xrightarrow{\ n\ } (k^{sep})^* \longrightarrow 0$$

we have a long exact sequence

$$0 \longrightarrow \mu_n \cap k \longrightarrow k^* \xrightarrow{\ n\ } k^* \xrightarrow{\ \delta\ } H^1(G_k, \mu_n) \longrightarrow H^1(G_k, (k^{sep})^*) = 0$$

Preliminaries

Definition 0.1. A **topological group** is a group G endowed with a topology such that the maps

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,h) & \mapsto & gh \end{array} \quad \text{and} \quad \begin{array}{ccc} G & \longrightarrow & G \\ g & \mapsto & g^{-1} \end{array}$$

are continuous.

$$G \times G \to G$$

both multiplication and taking inverses are continuous.

Remark. Let $L_a : G \to G$, given by $g \mapsto ag$, denote the left multiplication map. Then L_a is continuous. This is because we can write L_a as a composition of continuous maps $G \xrightarrow{g \mapsto (a,g)} G \times G \xrightarrow{(g,h) \mapsto gh} G$. In fact, L_a is a homeomorphism with inverse $L_{a^{-1}}$.

Lemma 0.1. *Let H be a subgroup of G.*

1. *If H is open, then H is closed.*
2. *If H is closed of finite index, then H is open.*

Proof. Let S be a set of coset representatives of H. Then $G \backslash H = \bigcup_{\sigma \in S \backslash \{e\}} \sigma H$. Each σH is open since H is open L_σ is a homeomorphism, and therefore the union $G \backslash H$ is open, which implies H is closed. The proof is nearly the same for (2) as it is for (1), but we need H to be of finite index since a union of infinitely many closed sets need not be closed. □

Definition 0.2. A **neighbourhood base** at $g \in G$ is a set of neighbourhoods $\mathcal{N}$ of g such that every open neighbourhood U of g contains some $V \in \mathcal{N}$.

Krull Topology

Definition 0.3. We say that a field extension Ω/K is a Galois extension if it is separable and for every K-linear embedding $\sigma \colon \Omega \to \overline{K}$ we have $\sigma(\Omega) = \Omega$ (so σ is a k-automorphism of Ω). The **Galois group** $\mathrm{Gal}(\Omega/K)$ of Ω/K is the set of all automorphisms of Ω which fix K.

Let E/K be a finite Galois extension. The fundamental theorem of Galois Theory gives us a *one-to-one correspondence* between fields L, where $K \subset L \subset E$, and subgroups of $\mathrm{Gal}(E/K)$. More explicitely, for any subgroup H of $\mathrm{Gal}(E/K)$, the corresponding fixed field, denoted E^H, is the set of all elements in E fixed by H; and for any field L, where $K \subset L \subset E$, the corresponding subgroup is $\mathrm{Aut}(E/L)$, that is, the set of all automorphisms in $\mathrm{Gal}(E/K)$ which fix L. For infinite extensions, this one-to-one correspondence breaks down, as demonstrated in the next example.

Example 0.2. Let $\Omega = \mathbb{Q}(\sqrt{p} \mid p \text{ is prime})$ and $G = \mathrm{Gal}(\Omega/\mathbb{Q})$. Then $\Omega/\mathbb{Q}$ is a Galois extension with Galois group G. For each prime number p, let σ_p by the unique element of G which maps $\sqrt{p}$ to $-\sqrt{p}$, and fixes everything else. Now consider the subgroup H of G generated by the σ_p's. Notice that $H \neq G$ since H does not contain the element $\sigma \in G$ which maps $\sqrt{p}$ to $-\sqrt{p}$ for all prime numbers p. However, we have

$$\Omega^H = \Omega^G = \mathbb{Q}.$$

Indeed, let $\alpha \in \Omega^H$. In particular, $\alpha \in \Omega$, so it is algebraic over $\mathbb{Q}$. This implies $\mathbb{Q}(\alpha)/\mathbb{Q}$ is finite, hence $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})$ for some primes $p_1, \ldots, p_k$. Since $\sigma_{p_1}, \ldots, \sigma_{p_k} \in H$, and since they generate $\mathrm{Gal}(E/\mathbb{Q})$, we conclude that $\alpha \in \mathbb{Q}$, by classical Galois theory for finite extensions.

In order to get a Galois correspondence for infinite extensions, we introduce a topology on G.

Definition 0.4. Let Ω/F be a Galois extension (possibly infinite). The **Krull topology** on Ω/F is the unique topology such that for all $\sigma \in \mathrm{Gal}(\Omega/F)$, the family of subsets

$$\{\sigma \mathrm{Gal}(\Omega/L) \mid \sigma \in \mathrm{Gal}(L/F),\ L/F \text{ is a finite Galois extension, and } L \subseteq \Omega\}$$

is a neighbourhood base at σ.

We may now state the fundamental theorem of Galois theory.

Theorem 0.2. *Let Ω/F be a Galois extension. Then there exist one-to-one correspondences between the following sets:*

1. *The set of subfields E of Ω containing F and the set of closed subgroups of $Gal(\Omega/F)$.*
2. *The set of subfields K of Ω containing F such that the degree of the extension K/F is finite and the set of open subgroups of $\mathrm{Gal}(\Omega/F)$.*
3. *The set of subfields L of Ω containing F such that L/F is a finite Galois extension and the set of open normal subgroups of $\mathrm{Gal}(L/F)$.*

In all cases, the correspondence is given by $E \mapsto \mathrm{Gal}(\Omega/E)$ and $H \mapsto \Omega^H$. Moreover, if H is an open normal subgroup of $\mathrm{Gal}(\Omega/F)$, then we have

$$\mathrm{Gal}(\Omega^H/F) \cong \mathrm{Gal}(\Omega/F)/H.$$

In particular, for any finite Galois subextension L/F of Ω/F, we have

$$\mathrm{Gal}(\Omega/F)/\mathrm{Gal}(\Omega/L) \cong \mathrm{Gal}(L/F).$$

The Galois Group as a Profinite Group

Let Ω/K be an infinite Galois extension and let L be a field such that $K \subset L \subset \Omega$ and L/K is a finite Galois extension. Denote $G := \mathrm{Gal}(\Omega/K)$ and $H := \mathrm{Gal}(\Omega/L)$. Then H is a normal subgroup of G, and $\mathrm{Gal}(L/K) \cong G/H$. In particular, since L/K is finite, H is of finite index in G. We have a canonical homorphism $G \to G/H \cong \mathrm{Gal}(L/K)$, given by $\sigma \mapsto \sigma_{|L}$. Therefore, we have a homomorphism from G to the inverse limit of the (inversely) directed family of normal subgroups with finite index:

$$\varphi : G \to \lim_{H \in \mathcal{F}} G/H,$$

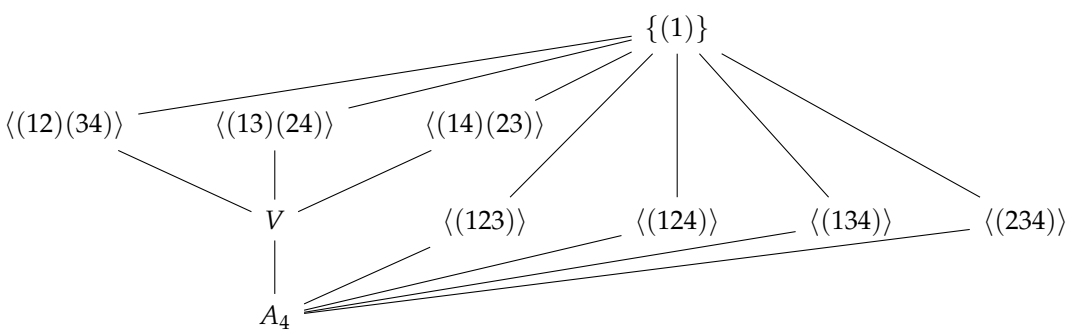
where $\mathcal{F}$ is the family of Galois groups as above.

Proposition 0.1. *The homomorphism $\varphi : G \to \lim_{H\in\mathcal{F}} G/H$ is an isomorphism.*

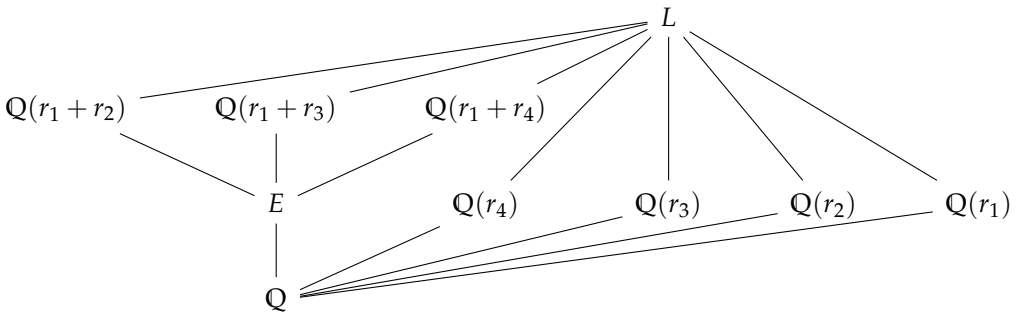
Proof. The map is obviously injective. For surjectivity, let $\{\sigma_L\} \in \lim_{H\in\mathcal{F}} G/H$. Let $\alpha \in \Omega$ and let E be the smallest Galois extension E/K, where $K \subset E \subset \Omega$, such that $\alpha \in E$. Define $\sigma(\alpha) := \sigma_E(\alpha)$. The map is well-defined and lies in G. □

The following examples demonstrates why it's very difficult to construct an element in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Example 0.3. Let $f(T) = T^4 + 8T + 12 = (T - r_1)(T - r_2)(T - r_3)(T - r_4)$, L be the splitting field of $f(T)$ over $\mathbb{Q}$, and E be the field given by $\mathbb{Q}(r_1r_2 + r_3r_4)$. Then $\mathbb{Q} \subset E \subset L$ and $E/\mathbb{Q}$ and $L/\mathbb{Q}$ are both Galois extensions. Below is the lattice of subgroups of $\mathrm{Gal}(L/\mathbb{Q}) \cong A_4$:



And here is the corresponding lattice of fields:



If we want to construct an element in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, then we certainly need to start with constructing an element σ_E in $\mathrm{Gal}(E/\mathbb{Q})$. After we construct σ_E in $\mathrm{Gal}(E/\mathbb{Q})$, we then then need to construct an element σ_L in $\mathrm{Gal}(L/\mathbb{Q})$ which is compatible with σ_E. Here's an example: let $\sigma_E = (r_1, r_2, r_3)$ and let $\sigma_L = (r_1, r_2, r_3)(r_1, r_2)(r_3, r_4)$. The problem with this example though is that we used the roots r_1, r_2, r_3, r_4 of f to describe σ_E. For instance, let $g(T) = \prod_{i=1}^{n}(T - s_i)$ be a polynomial such that its splitting field contains L. Then we would need to rewrite σ_E in terms of the roots $s_1, \ldots, s_n$.

The open normal subgroup in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ which corresponds to L is $\mathrm{Gal}(\bar{\mathbb{Q}}/L)$. The open subgroup in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ which corresponds to $\mathbb{Q}(r_4)$ is $\bigcup_{\sigma\in S_3} \sigma\mathrm{Gal}(\bar{\mathbb{Q}}/L)$, where we choose σ to be an in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma_{|L}$ permutes the roots r_1, r_2, and r_3.

Γ-sets, Γ-groups, and Γ-modules

Definition 0.5. Let Γ be a profinite group. A left action of Γ on a discrete topological space A is called **continuous** if for all $a \in A$, the set

$$\mathrm{Stab}_\Gamma(a) = \{\sigma \in \Gamma \mid \sigma \cdot a = a\}$$

is an open subgroup of Γ.

Lemma 0.3. *This is equivalent to ask for the map*

$$\Gamma \times A \to A$$
$$(\sigma, a) \mapsto \sigma \cdot a$$

to be continuous.

Proof. We need to show that the inverse image of an open set in A is open in $\Gamma \times A$. Since A is discrete, every open set in A is a union of singleton sets, so we may as well look at the inverse image of a singleton set, say $\{b\}$, where $b \in A$. For each $a \in A$ we want to show that the set of all $\sigma \in \Gamma$ such that $\sigma \cdot a = b$ is open, no matter which a you choose. If $a = b$, then by assumption, the set of all σ such that $\sigma \cdot a = b$ is an open subgroup. So suppose $a \neq b$. Let σ be an element in Γ such that $\sigma \cdot a = b$ (if there isn't one, then the set is empty, hence open). Then the set

$$(Stab_\Gamma(b))\sigma = \{\tau\sigma \mid \tau \in Stab_\Gamma(b)\}$$

is an open neighborhood of σ. Since σ is arbitrary, we are done.

□

Definition 0.6. Discrete topological spaces with a continuous left action of Γ are called Γ-**sets**. A group A which is also a Γ-set is called a Γ-**group** if Γ acts by group morphisms, i.e.

$$\sigma \cdot (ab) = (\sigma \cdot a)(\sigma \cdot b) \text{ for } \sigma \in \Gamma,\ a, b \in A$$

A Γ-group which is commutative is called a Γ-**module**. A **morphism** of Γ-sets (resp. Γ-groups, Γ-modules) is a map (resp. a group morphism) $f : A \to A'$ satisfying the following property:

$$f(\sigma \cdot a) = \sigma \cdot f(a) \text{ for all } \sigma \in \Gamma, \text{ and } a \in A.$$

Example 0.4.

1. If Γ is a finite group, then any discrete topological set A on which Γ acts on the left is a Γ-set. This is because Γ is profinite, which makes it discrete if Γ is finite. So any map
$$\Gamma \times A \to A$$
is continuous.
2. Any discrete topological set A on which Γ acts trivially is a Γ-set. In this case, the stabilizer of any point in A is the entire set Γ.
3. Let Ω/K be a Galois extension and let G_Ω denote its Galois group. Then the map
$$G_\Omega \times \Omega \to \Omega$$
$$(\sigma, \alpha) \mapsto \sigma(\alpha)$$
endows Ω with the structure of a G_Ω-module. This is an important example. Given any $\alpha \in \Omega$, the stabilizer of α for the action of G_Ω is equal to the open subgroup $\mathrm{Gal}(\Omega/K(\alpha))$.
4. Let V be a K-vector space, and let us denote by V_Ω the tensor product $\Omega \otimes_K V$. Then the action of G_Ω on V_Ω defined on elementary tensors by
$$\sigma \cdot (\alpha \otimes v) = \sigma(\alpha) \otimes v \text{ for all } v \in V,\ \alpha \in \Omega$$
is continuous, and therefore endows V_Ω with the structure of a G_Ω-module.
5. Let V and W be two K-vector spaces of dimensions n and m respectively. Then G_Ω acts on $\mathrm{Hom}_\Omega(V_\Omega, W_\Omega)$ as follows: Given $\varphi \in \mathrm{Hom}_\Omega(V_\Omega, W_\Omega)$, set
$$(\sigma \cdot \varphi)(x) = \sigma \cdot (\varphi(\sigma^{-1} \cdot x)) \text{ for all } x \in V_\Omega.$$
A choice of bases induces an isomorphism $\mathrm{Hom}_\Omega(V_\Omega, W_\Omega) \simeq M_{m\times n}(\Omega)$, and the corresponding action of G_Ω on $M_{m\times n}(\Omega)$ is simply the action entrywise. To see how this works take the case $\Omega = \mathbb{C}$, $K = \mathbb{R}$, with V and W both two dimensional $\mathbb{R}$-vector spaces. Let $\{e_1, e_2\}$ be a basis for V, $\{f_1, f_2\}$ be a basis for W, and let $\varphi \in \mathrm{Hom}_\Omega(V_\Omega, W_\Omega)$. Then $\{1 \otimes e_1, 1 \otimes e_2\}$ will be a basis for $\mathbb{C} \otimes_\mathbb{R} \mathbb{V}$, and $\{1 \otimes f_1, 1 \otimes f_2\}$ will be a basis for $\mathbb{C} \otimes_\mathbb{R} \mathbb{W}$. To determine the matrix which corresponds to φ, we see where φ maps the basis vectors:
$$\varphi(1 \otimes e_1) = a_{11} \otimes f_1 + a_{21} \otimes f_2$$
$$\varphi(1 \otimes e_2) = a_{12} \otimes f_1 + a_{22} \otimes f_2$$

where $a_{ij} \in \mathbb{C}$. So the matrix which corresponds to φ is $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$. To determine the matrix which corresponds to $\sigma \cdot \varphi$, we see where $\sigma \cdot \varphi$ maps the basis vectors

$$\begin{aligned}(\sigma \cdot \varphi)(1 \otimes e_1) &= \sigma(\varphi(\sigma^{-1}(1) \otimes e_1) \\ &= \sigma(\varphi(1 \otimes e_1) \\ &= \sigma(a_{11}) \otimes f_1 + \sigma(a_{21}) \otimes f_2\end{aligned}$$

$$\begin{aligned}(\sigma \cdot \varphi)(1 \otimes e_2) &= \sigma(\varphi(\sigma^{-1}(1) \otimes e_2) \\ &= \sigma(\varphi(1 \otimes e_2) \\ &= \sigma(a_{12}) \otimes f_1 + \sigma(a_{22}) \otimes f_2\end{aligned}$$

So the matrix which corresponds to $\sigma \cdot \varphi$ is $\left(\begin{smallmatrix} \sigma(a_{11}) & \sigma(a_{12}) \\ \sigma(a_{21}) & \sigma(a_{22}) \end{smallmatrix}\right)$. Going back to the general case, after choosing bases for V and W, we have the induced isomorphism $\mathrm{Hom}_\Omega(V_\Omega, W_\Omega) \simeq M_{m\times n}(\Omega)$. Then the stabilizer for the action of G_Ω of a given matrix M in $M_{m\times n}(\Omega)$ is equal to the open subgroup $\mathrm{Gal}_\Omega(\Omega/K)$, where K is the subfield of Ω generated by the entries of M. Indeed $\sigma \in G_\Omega$ will act trivially on M if and only if it acts trivially on the entries of M. So we have a continuous G_Ω action.

6. The action in the previous example also induces an action on G_Ω on $\mathbf{GL}(V_\Omega)$. It is an action by group automorphisms, so that $\mathbf{GL}(V_\Omega)$ is a Γ_Ω-group. In particular, $GL_n(\Omega)$ is a Γ_Ω-group. The same is true for other matrix groups such as $SL_n(\Omega)$ and $O_n(\Omega)$. Indeed, we already have a continuous action, we need to check that

$$\sigma \cdot (ab) = (\sigma \cdot a)(\sigma \cdot b) \text{ for } \sigma \in G,\ a, b \in A$$

For the case $n = 2$, we have

$$\begin{pmatrix} \sigma \cdot a & \sigma \cdot b \\ \sigma \cdot c & \sigma \cdot d \end{pmatrix} \begin{pmatrix} \sigma \cdot a' & \sigma \cdot b' \\ \sigma \cdot c' & \sigma \cdot d' \end{pmatrix} = \begin{pmatrix} (\sigma \cdot a)(\sigma \cdot a') + (\sigma \cdot b)(\sigma \cdot c') & (\sigma \cdot a)(\sigma \cdot b') + (\sigma \cdot b)(\sigma \cdot d') \\ (\sigma \cdot c)(\sigma \cdot a') + (\sigma \cdot d)(\sigma \cdot c') & (\sigma \cdot c)(\sigma \cdot b') + (\sigma \cdot d)(\sigma \cdot d') \end{pmatrix} = \sigma \cdot \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

The cases where $n > 2$ can also be verified easily. This shows that $GL_n(\Omega)$ is a G_Ω-group. For $SL_n(\Omega)$ to be a G_Ω-group, we also need to check that the resulting matrix lies in $SL_n(\Omega)$. For the case $n = 2$, we have

$$\begin{aligned}\left|\begin{pmatrix} \sigma \cdot a & \sigma \cdot b \\ \sigma \cdot c & \sigma \cdot d \end{pmatrix}\right| &= (\sigma \cdot a)(\sigma \cdot d) - (\sigma \cdot c)(\sigma \cdot b) \\ &= \sigma \cdot (ad - bc) \\ &= \sigma(1) \\ &= 1.\end{aligned}$$

The cases where $n > 2$ can also be verified easily.

7. $GL_1(\Omega)$ is sometimes denoted $\Omega^\times$, i.e., the multiplicative group of units. Let $\mu_n(\Omega)$ be the group of n^{th} roots of 1 in Ω. Then $\mu_n(\Omega)$ is a G_Ω-submodule of $\Omega^\times$.

Lemma 0.4. *Let Γ be a profinite group, and let A be a discrete topological set on which Γ acts on the left. Then the action of Γ on A is continuous if and only if we have*

$$A = \bigcup_{U \in \mathcal{N}} A^U$$

where $\mathcal{N}$ denotes the set of open normal subgroups of Γ.

Proof. Here, A^U means

$$\{a \in A \mid \sigma \cdot a = a \text{ for all } \sigma \in U\}$$

So given an $a \in A$, we need to show that it belongs to some A^U, where U is an open normal subgroup of Γ. Since the action is continuous, we know that the stabilizer of a is an open subgroup which contains 1, but it isn't necesarrily normal. However, every neighborhood of 1 contains an open normal subgroup. Conversely, assume that we have

$$A = \bigcup_{U \in \mathcal{N}} A^U$$

By assumption, there exists $U \in \mathcal{N}$ such that $a \in A^U$. Therefore, for all $\sigma \in U$, we have $\sigma \cdot a = a$. If now $\tau \in Stab_\Gamma(a)$, then $\tau\sigma \in Stab_\Gamma(a)$ for all $\sigma \in U$, Thus

$$\bigcup_{\tau \in Stab_\Gamma(a)} \tau U \subset Stab_\Gamma(a)$$

Since $1 \in U$, the other inclusion holds as well, and we get

$$\bigcup_{\tau \in Stab_\Gamma(a)} \tau U = Stab_\Gamma(a)$$

It follows that $Stab_\Gamma(a)$ is open.

□

Part II
Cohomology Definition

We will split this up into two sections. The first section deals with cohomology with coefficients in a Γ-module, using additive notation. The second section generalizes this to deal with the case where the coefficient is a Γ-set or Γ-group, using multiplicative notation.

1 Cohomology with coefficients in a Γ-module.

Definition 1.1. The set of maps $f : \Gamma^n \to A$ is denoted by $C^n(\Gamma; A)$ and is called the **n-cochains** on Γ with values in A. Define the maps $d_n : C^n(\Gamma; A) \to C^{n+1}(\Gamma; A)$ as follows:

$$d_0(a)_\sigma = \sigma \cdot a - a \qquad \sigma \in \Gamma$$

and for all $n \geq 1$ by $(\sigma_1, \ldots, \sigma_{n+1} \in \Gamma)$

$$d_n(\alpha)_{\sigma_1,\ldots,\sigma_{n+1}} = \sigma_1 \cdot \alpha_{\sigma_2,\ldots,\sigma_{n+1}} + \sum_{i=1}(-1)^i \alpha_{\sigma_1,\ldots,\sigma_i\sigma_{i+1},\ldots,\sigma_{n+1}} + (-1)^{n+1}\alpha_{\sigma_1,\ldots,\sigma_n}$$

For now on, we will drop the index n in d_n when it is clear. One readily verifies that $dd = 0$ and the **nth cohomology group** $(n \geq 0)$ of Γ with **coefficients** in A, $H^n(\Gamma; A)$, is defined by

$$H^n(\Gamma; A) = \frac{(\ker d : C^n(\Gamma; A) \to C^{n+1}(\Gamma; A))}{(\mathrm{im} d : C^{n-1}(\Gamma; A) \to C^n(\Gamma; A))}$$

where we set $C^n(\Gamma; A) = 0$ if $n < 0$.

This is nothing but the cohomology of the chain complex:

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow C^0(\Gamma, A) \xrightarrow{d} C^1(\Gamma, A) \xrightarrow{d} C^2(\Gamma, A) \xrightarrow{d} \cdots$$

Here is how it looks at the level of elements, where $a \in C^0(\Gamma; A) = A$, $\alpha \in C^1(\Gamma; A)$, $\beta \in C^2(\Gamma; A)$.

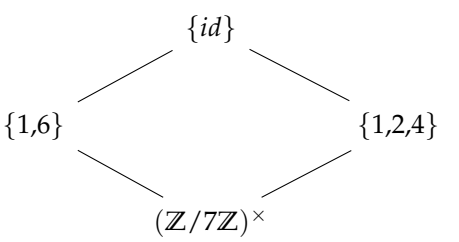
$$d(a)_\sigma = \sigma \cdot a - a$$
$$d(\alpha)_{\sigma,\tau} = \sigma \cdot \alpha_\tau - \alpha_{\sigma\tau} + \alpha_\sigma$$
$$d(\beta)_{\sigma,\tau,\gamma} = \sigma \cdot \beta_{\tau,\gamma} - \beta_{\sigma\tau,\gamma} + \beta_{\sigma,\tau\gamma} - \beta_{\sigma,\tau}$$

Suppose $\sigma \in \Gamma$ has order n. Using the cocycle relation, let's figure out what α_σ looks like:

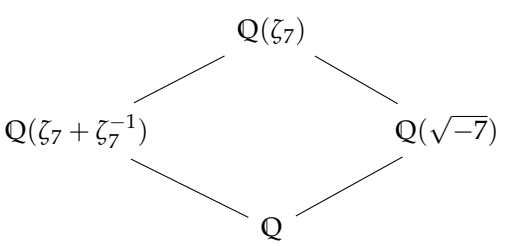
$$\alpha_\sigma = \alpha_\sigma$$
$$\alpha_{\sigma^2} = \alpha_\sigma + \sigma \cdot \alpha_\sigma$$
$$\alpha_{\sigma^3} = \alpha_\sigma + \sigma \cdot \alpha_\sigma + \sigma^2 \cdot \alpha_\sigma$$
$$\cdots$$
$$0 = \alpha_1 = (1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1})\alpha_\sigma$$

The fact that $\alpha_1 = 0$ follows easily from the cocycle relation. In the group ring $\mathbb{Z}[\Gamma]$, the element $N_\Gamma = \sum_{\sigma \in \Gamma} \sigma$ is called the **norm** (or **trace**) of $\mathbb{Z}[\Gamma]$. Think of this as something formal which becomes concrete when applied to an element in A.

Example 1.1. Consider the field extension $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. Let Γ be the corresponding Galois group $Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times$, and let A be $\mathbb{Q}(\zeta_7)^\times$. Below is the diagram of all subgroups of $(\mathbb{Z}/7\mathbb{Z})^\times$, written upside down.



And the corresponding lattice of intermediate fields in $\mathbb{Q}(\zeta_7)/\mathbb{Q}$:



A 1-cocycle α is determined by its value on the generator $\sigma \in \Gamma$. By the cocycle relation we have

$$(\sigma^6 \cdot \alpha_\sigma)(\sigma^5 \cdot \alpha_\sigma)(\sigma^4 \cdot \alpha_\sigma)(\sigma^3 \cdot \alpha_\sigma)(\sigma^2 \cdot \alpha_\sigma)(\sigma \cdot \alpha_\sigma)\alpha_\sigma = 1$$

This expression is exactly the (Galois) norm of α_σ. Hence, a 1-cocycle must send the generator σ to an element of norm one in A.

Now in the more general caseσ generates a cyclic subgroup of Γ of order n, which will denote by Γ_n. We are going to want to relate cohomology information between Γ_n and Γ. So we can only speak about relative norms here.

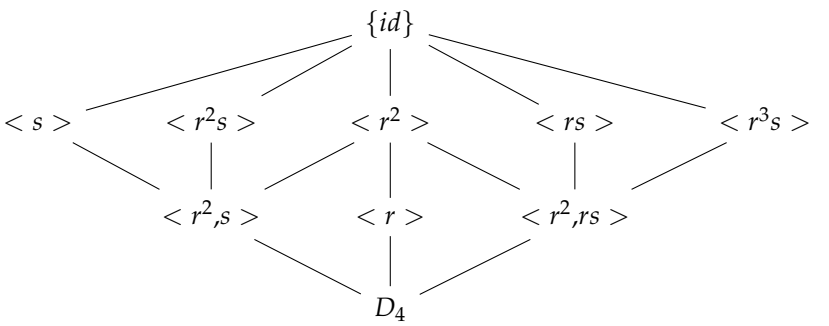
Example 1.2. The extension $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ is Galois since:

1. Any extension of $\mathbb{Q}$ is separable.
2. It is the splitting field over $\mathbb{Q}$ for $x^4 - 2$.

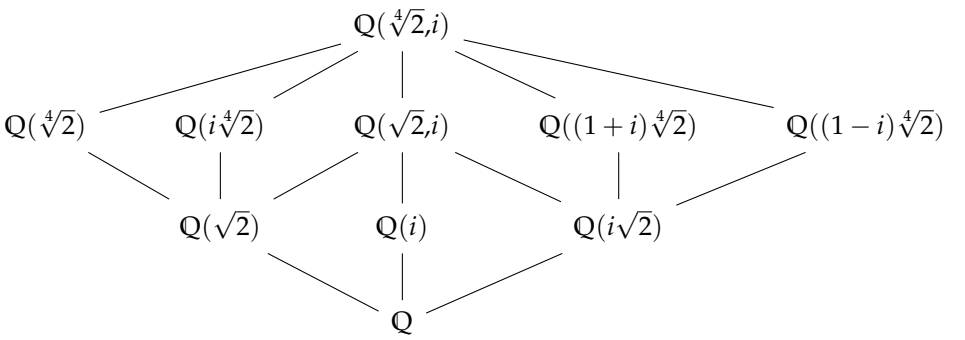
The Galois group for this extension is isomorphic to

$$D_4 = < r, s \mid r^4 = s^2 = 1,\ srs = r^{-1} > .$$

Below is the diagram of all subgroups of D_4, written upside down.



The lattice of intermediate fields in $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ looks the same:



$\mathbb{Q}(i) : \mathbb{Q}$ has degree 2, so its corresponding subgroup H in D_4 has index 2. Since $r(i) = i$, $< r >$ is a subgroup fixing i with index $8/4 = 2$, so $H =< r >$. Thus $Q(i)$ corresponds to $< r >$. The following table shows the 8 different automorphisms of $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$:

σ	id	r	r^2	r^3	s	rs	r^2s	r^3s
$\sigma(\sqrt[4]{2})$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

Let $\Gamma = Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ and $A = \mathbb{Q}(\sqrt[4]{2}, i)^\times$. A 1-cocycle α is completely determined by its values on r and s. Since s has order 2, r has order 4, we must have

$$1 = (r^3 \cdot \alpha_r)(r^2 \cdot \alpha_r)(r \cdot \alpha_r)\alpha_r = (s \cdot \alpha_s)\alpha_s$$

Since the subgroup $< r >$ fixes $\mathbb{Q}(i)$, and the subgroup $< s >$ fixes $\mathbb{Q}(\sqrt[4]{2})$, we see that if α_r belonged to $\mathbb{Q}(i)$, then we must have $\alpha_r^4 = 1$, and if α_s belonged to $\mathbb{Q}(\sqrt[4]{2})$, then $\alpha_s^2 = 1$. These have obvious solutions. We can't say much else until later on.

Let α be a 2-cocycle. Using the 2-cocycle relations, we easily get

$$\sigma \cdot \alpha_{1,1} = \alpha_{\sigma,1} \quad a_{1,\sigma} = a_{1,1} \quad a_{\sigma^{-1},\sigma} = a_{\sigma,\sigma^{-1}}$$

It may be helpful at first to view a 2-cocycle using a table like this.

α	1	σ	τ	γ	$\sigma\tau$	$\tau\gamma$	$\dots$
1	$\alpha_{1,1}$	$\alpha_{1,1}$	$\alpha_{1,1}$	$\alpha_{1,1}$	$\alpha_{1,1}$	$\alpha_{1,1}$	$\dots$
σ	$\sigma \cdot \alpha_{1,1}$	$\alpha_{\sigma,\sigma}$	$\sigma \cdot a_{\tau,\gamma} - a_{\sigma\tau,\gamma} + a_{\sigma,\tau\gamma}$	$\alpha_{\sigma,\gamma}$	$\alpha_{\sigma,\sigma\tau}$	$\alpha_{\sigma,\tau\gamma}$	$\dots$
τ	$\tau \cdot \alpha_{1,1}$	$\alpha_{\tau,\sigma}$	$\alpha_{\tau,\tau}$	$\alpha_{\tau,\gamma}$	$\alpha_{\tau,\sigma\tau}$	$\alpha_{\tau,\tau\gamma}$	$\dots$
γ	$\gamma \cdot \alpha_{1,1}$	$\alpha_{\gamma,\sigma}$	$\alpha_{\gamma,\tau}$	$\alpha_{\gamma,\gamma}$	$\alpha_{\gamma,\sigma\tau}$	$\alpha_{\gamma,\tau\gamma}$	$\dots$
$\sigma\tau$	$\sigma\tau \cdot \alpha_{1,1}$	$\alpha_{\sigma\tau,\sigma}$	$\alpha_{\sigma\tau,\tau}$	$\alpha_{\sigma\tau,\gamma}$	$\alpha_{\sigma\tau,\sigma\tau}$	$\alpha_{\sigma\tau,\tau\gamma}$	$\dots$
$\tau\gamma$	$\tau\gamma \cdot \alpha_{1,1}$	$\alpha_{\tau\gamma,\sigma}$	$\alpha_{\tau\gamma,\tau}$	$\alpha_{\tau\gamma,\gamma}$	$\alpha_{\tau\gamma,\sigma\tau}$	$\alpha_{\tau\gamma,\tau\gamma}$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

Definition 1.2. We say a 2-cocycle α is normalized if $\alpha_{1,1} = 0$.

It turns out that every 2-cocycle is cohomologous to a normalized one: Given an arbitrary 2-cocycle α, define the 1-cochain β as

$$\beta_\sigma = \alpha_{\sigma,\sigma}$$

Then $\alpha - d\beta$ is a cocycle which is cohomologous to α and

$$(\alpha - d\beta)_{1,1} = \alpha_{1,1} - 1 \cdot \alpha_{1,1} + \alpha_{1^2,1^2} - \alpha_{1,1} = 0$$

Thus, we may assume that the representative $\alpha \in C^2(G, A)$ of the cohomology class $[\alpha] \in H^2(G, A)$, has values

$$\alpha_{1,h} = 1 \quad \text{and} \quad \alpha_{g,1} = 1 \quad \forall g, h \in G$$

2 Functor of pairs (Γ, A)

Definition 2.1. A **morphism of pairs** $(\Gamma, A) \mapsto (\Gamma', A')$ is given by a pair of maps ϕ and f,

$$\Gamma \leftarrow \Gamma' : \phi \qquad \text{and} \qquad f : A_\phi \to A'$$

where ϕ is a group homomorphism, and f is a homomorphism of Γ'-modules, and A_ϕ means A with the Γ' action $\star$ induced by ϕ:

$$\sigma \star a = \phi(\sigma) \cdot a$$

A morphism of pairs induces a map

$$H^r(\Gamma, A) \to H^r(\Gamma', A')$$
$$[\alpha] \mapsto [f_*(\alpha)]$$

got by composing the map $H^r(\Gamma, A) \to H^r(\Gamma', A_\phi)$ induced by ϕ with the map $H^r(\Gamma', A_\phi) \to H^r(\Gamma', A')$ induced by f. We thus consider $H^r(\Gamma, A)$ as a functor of pairs (Γ, A).

So for example, if $\alpha \in Z^1(\Gamma, A)$ has values at $\sigma \in \Gamma$ given by $\alpha_\sigma = \alpha_\sigma$, then $f_*(\alpha) \in Z^1(\Gamma', A_\phi)$ has values at $\sigma' \in \Gamma'$ given by $f_*(\alpha)_{\sigma'} = f(\alpha_{\phi(\sigma')})$. That $f_*(\alpha)$ really is a 1-cocycle follows from

$$\begin{aligned} f_*(\alpha)_{\sigma'\tau'} &= f(\alpha_{\phi(\sigma'\tau')}) \\ &= f(\alpha_{\phi(\sigma')\phi(\tau')}) \\ &= f(\alpha_{\phi(\sigma')} + \phi(\sigma') \cdot \alpha_{\phi(\tau')}) \\ &= f(\alpha_{\phi(\sigma')}) + f(\phi(\sigma') \cdot (\alpha_{\phi(\tau')})) \\ &= f(\alpha_{\phi(\sigma')}) + \sigma' \cdot f(\alpha_{\phi(\tau')}) \end{aligned}$$

2.1 Vanishing criterion for cohomology of finite groups

Theorem 2.1. *Suppose G is a finite group with $|G| = m$ and suppose A is a G-module. If $\overline{\alpha} \in H^n(G, A)$ with $n \geq 1$, then $\overline{m\alpha} = \overline{0}$.*

Proof. Let $\alpha \in Z^n(G, A)$ be an n-cocycle in the class $\overline{\alpha}$. We will show that $m\alpha$ is a coboundary. Since α is an n-cocycle, we have:

$$\sigma_1 \cdot \alpha_{\sigma_2,\ldots,\sigma_{n+1}} + \sum_{i=1}(-1)^i \alpha_{\sigma_1,\ldots,\sigma_i\sigma_{i+1},\ldots,\sigma_{n+1}} + (-1)^{n+1}\alpha_{\sigma_1,\ldots,\sigma_n} = 0$$

Define $\Pi \in C^{n-1}(G, A)$ by

$$\Pi_{\sigma_1,\ldots,\sigma_{n-1}} = \sum_{\sigma \in G} \alpha_{\sigma_1,\ldots,\sigma_{n-1},\sigma}$$

By summing over σ_{n+1}, the cocycle condition above gives:

$$\sigma_1 \cdot \Pi_{\sigma_2,\ldots,\sigma_n} + \sum_{i=1}(-1)^i \Pi_{\sigma_1,\ldots,\sigma_i\sigma_{i+1},\ldots,\sigma_n} + (-1)^n \Pi_{\sigma_1,\ldots,\sigma_{n-1}} + (-1)^{n+1} m\alpha_{\sigma_1,\ldots,\sigma_n} = 0$$

To compute the one before last term on the right, we have used the fact that if σ_{n+1} runs through G, so does $\sigma_n\sigma_{n+1}$. Thus we obtain

$$d((-1)^n \Pi) = m\alpha$$

□

Example 2.1. Let's see how this works in the case $n = 3$.

$$\begin{aligned} g \cdot \Pi_{h,k} &= g \cdot \alpha_{h,k,x_1} + g \cdot \alpha_{h,k,x_2} + \cdots + g \cdot \alpha_{h,k,x_i} + \cdots + g \cdot \alpha_{h,k,x_m} && G = \{x_1, x_2, \ldots, x_i, \ldots, x_m\} \\ -\Pi_{gh,k} &= -\alpha_{gh,k,x_1} - \alpha_{gh,k,x_2} - \cdots - \alpha_{gh,k,x_i} - \cdots - \alpha_{gh,k,x_m} \\ +\Pi_{g,hk} &= \alpha_{g,hk,x_1} + \alpha_{g,hk,x_2} + \cdots + \alpha_{g,hk,x_i} + \cdots + \alpha_{g,hk,x_m} \\ -\Pi_{g,h} &= -\alpha_{g,h,kx_1} + \alpha_{g,h,kx_2} + \cdots + \alpha_{g,h,kx_i} + \cdots + \alpha_{g,h,kx_m} && x_i \mapsto kx_i \text{ is invertible.} \\ (d(-\Pi))_{g,h,k} &= m\alpha_{g,h,k} \end{aligned}$$

2.2 Examples

2.2.1 Conjugation

Let G, H be groups with $H \subset G$. Then

$$H^r(H, A) \to H^r(gHg^{-1}, A) \quad g \in G$$
$$ghg^{-1} \mapsto h$$

$$\Gamma \leftarrow \Gamma' : \phi \qquad \text{and} \qquad f : A_\phi \to A'$$

2.2.2 Restriction-Corestriction Maps

If Γ' is a subgroup of Γ then there are maps

$$H^r(\Gamma, A) \underset{\text{corestriction}}{\overset{\text{restriction}}{\rightleftarrows}} H^r(\Gamma', A)$$

The restriction map is easy to as a specific case of the general map we constructed above. Suppose $\sigma \in \Gamma'$ but $\tau \notin \Gamma'$. If α is a 1-cocycle in $H^1(\Gamma, A)$

$$\alpha : \begin{array}{c|c|c|c|c} 1 & \sigma & \tau & \sigma\tau & \dots \\ \hline 0 & \alpha_\sigma & \alpha_\tau & \alpha_\sigma(\sigma \cdot \alpha_\tau) & \dots \end{array}$$

The restriction of α to $H^1(\Gamma', A)$ would look like this:

$$\begin{array}{c|c|c} 1 & \sigma & \dots \\ \hline 0 & \alpha_\sigma & \dots \end{array}$$

The corestriction map (also called the "transfer map") is defined only if the index $[\Gamma : \Gamma']$ is finite. When $r = 0$, the corestriction map is simply the norm or trace:

$$A^\Gamma \underset{\text{corestriction}}{\overset{\text{restriction}}{\rightleftarrows}} A^{\Gamma'}$$

$$a \mapsto \sum_{\sigma \in \{\text{coset reps for } \Gamma/\Gamma'\}} \sigma \cdot a$$

Example 2.2. Let's go back to the extension $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$, where we set identified $Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ with D_4 and then set Γ to be D_4 and $A = \mathbb{Q}(\sqrt[4]{2}, i)^\times$. Let Γ' be the subgroup $\langle r \rangle$, which is normal in D_4. Since $\langle r \rangle$ is normal in D_4, the cosets $D_4/\langle r \rangle$ actually form a group. And by Galois theory, this group is isomorphic to the Galois group $Gal(\mathbb{Q}(i)/\mathbb{Q})$. An explicit choice of coset representatives then is $\{1, s\}$. Given a 1-cocycle α in $H^1(\Gamma, A)$

1	r	r^2	r^3	s	rs	r^2s	r^3s
1	α_r	$\alpha_r(r \cdot \alpha_r)$	$\alpha_r(r \cdot \alpha_r)(r^2 \cdot \alpha_r)$	α_s	$\alpha_r(r \cdot \alpha_s)$	$\alpha_r(r \cdot \alpha_r)(r^2 \cdot \alpha_s)$	$\alpha_r(r \cdot \alpha_r)(r^2 \cdot \alpha_r)(r^3 \cdot \alpha_s)$

The restriction of this 1-cocycle in $H^1(\Gamma', A)$ is

1	r	r^2	r^3
1	α_r	$\alpha_r(r \cdot \alpha_r)$	$\alpha_r(r \cdot \alpha_r)(r^2 \cdot \alpha_r)$

Also, given a 0-cycle a in $H^0(\Gamma, A) = A^\Gamma$

$$a \in \mathbb{Q}^\times$$

The "restriction" of of this 0-cycle in $H^0(\Gamma', A) = A^{\Gamma'}$ is

$$a \in \mathbb{Q}(i)^\times$$

Using the coset representatives $\{1, s\}$, the corestriction from $H^0(\Gamma', A)$ to $H^0(\Gamma, A)$ is the norm map from $\mathbb{Q}(i)^\times$ to $\mathbb{Q}^\times$:

$$x + iy \mapsto (x + iy)(x - iy)$$

If we apply the corestriction map to the restriction of a we get a squaring map from $\mathbb{Q}^\times \to \mathbb{Q}^\times$:

$$a \mapsto a^2$$

Corollary. *If Γ is of finite cardinality m, then*

$$m \cdot H^r(\Gamma, A) = 0 \quad \textit{for } r \neq 0$$

Proof. Letting $\Gamma' = \{1\}$ we have

$$(\text{corestriction}) \circ (\text{restriction}) = [\Gamma : \Gamma'] = [\Gamma : \{1\}] = m$$

Since $H^r(\{1\}, A) = 0$ for $r \neq 0$, this composition is 0, as claimed. □

3 Nonabelian Cohomology

We begin by defining the 0^{th} cohomology set $H^0(G, A)$.

Definition 3.1. For any Γ-set A, we set

$$H^0(\Gamma, A) = A^\Gamma$$

If A is a Γ-group, this is a subgroup of A. The set $H^0(\Gamma, A)$ is called the **0^{th} cohomology set of Γ with coefficients in A.**

Next, we define the first cohomology set $H^1(G, A)$.

Definition 3.2. Let A be a Γ-group. A 1-cocycle of Γ with values in A is a *continuous* map $\alpha : \Gamma \to A$ such that

$$\alpha_{\sigma\tau} = \alpha_\sigma(\sigma \cdot \alpha_\tau) \quad \forall \sigma, \tau \in \Gamma$$

Sometimes we will write the cocycle like this:

$$\alpha : \begin{array}{c|c|c|c|c} 1 & \sigma & \tau & \sigma\tau & \dots \\ \hline \alpha_1 & \alpha_\sigma & \alpha_\tau & \alpha_\sigma(\sigma \cdot \alpha_\tau) & \dots \end{array}$$

We denote by $Z^1(\Gamma, A)$ the set of all 1-cocycles of Γ with values in A. The constant map:

$$1 : \begin{array}{c|c|c|c|c} 1 & \sigma & \tau & \sigma\tau & \dots \\ \hline 1 & 1 & 1 & 1 & \dots \end{array}$$

is an element of $Z^1(\Gamma, A)$, which is called the **trivial** 1-cocycle. Two 1-cocycles α,β are said to be **cohomologous** if there exists $a \in A$ satisfying

$$\beta_\sigma = a\alpha_\sigma(\sigma \cdot a^{-1}) \text{ for all } \sigma \in \Gamma$$

it is denoted $\alpha \sim \beta$, and it is easily checked to be an equivalence relation on $Z^1(\Gamma, A)$. We denote by $H^1(\Gamma, A)$ the quotient set

$$H^1(\Gamma, A) = Z^1(\Gamma, A)/\sim$$

So in $H^1(\Gamma, A)$,

$$\alpha : \begin{array}{c|c|c|c|c} 1 & \sigma & \tau & \sigma\tau & \dots \\ \hline \alpha_1 & \alpha_\sigma & \alpha_\tau & \alpha_\sigma(\sigma \cdot \alpha_\tau) & \dots \end{array}$$

$$\sim \beta : \begin{array}{c|c|c|c|c} 1 & \sigma & \tau & \sigma\tau & \dots \\ \hline a\alpha_1 a^{-1} & a\alpha_\sigma(\sigma \cdot a^{-1}) & a\alpha_\tau(\tau \cdot a^{-1}) & a\alpha_{\sigma\tau}(\sigma\tau \cdot a^{-1}) & \dots \end{array}$$

$$= \beta : \begin{array}{c|c|c|c|c} 1 & \sigma & \tau & \sigma\tau & \dots \\ \hline a\alpha_1 a^{-1} & a\alpha_\sigma(\sigma \cdot a^{-1}) & a\alpha_\tau(\tau \cdot a^{-1}) & a\alpha_\sigma(\sigma \cdot \alpha_\tau)(\sigma\tau \cdot a^{-1}) & \dots \end{array}$$

$$= \beta : \begin{array}{c|c|c|c|c} 1 & \sigma & \tau & \sigma\tau & \dots \\ \hline a\alpha_1 a^{-1} & a\alpha_\sigma(\sigma \cdot a^{-1}) & a\alpha_\tau(\tau \cdot a^{-1}) & a\alpha_\sigma\sigma \cdot (\alpha_\tau\tau \cdot a^{-1}) & \dots \end{array}$$

$$= \beta : \begin{array}{c|c|c|c|c} 1 & \sigma & \tau & \sigma\tau & \dots \\ \hline a\alpha_1 a^{-1} & a\alpha_\sigma(\sigma \cdot a^{-1}) & a\alpha_\tau(\tau \cdot a^{-1}) & a\alpha_\sigma\sigma \cdot (a^{-1}a\alpha_\tau(\tau \cdot a^{-1})) & \dots \end{array}$$

$$= \beta : \begin{array}{c|c|c|c|c} 1 & \sigma & \tau & \sigma\tau & \dots \\ \hline a\alpha_1 a^{-1} & a\alpha_\sigma(\sigma \cdot a^{-1}) & a\alpha_\tau(\tau \cdot a^{-1}) & a\alpha_\sigma(\sigma \cdot a^{-1})\sigma \cdot (a\alpha_\tau(\tau \cdot a^{-1})) & \dots \end{array}$$

Remark. If G acts trivially on A, a 1-cocycle is just a continous morphism $a : G \to A$.

4 Extra

There are two ways of writing elements in $\mathbb{Z}[G \times G]$, depending on whether we think of $\mathbb{Z}[G \times G]$ as a free $\mathbb{Z}$-module or a free $\mathbb{Z}[G]$-module. The first way is $\sum n_{g,h}(g,h)$, where the sum ranges over $g,h \in G$ and $n_{g,h} \in \mathbb{Z}$. The second way is $\sum a_g(1,g)$, where the sum ranges over $g \in G$ and $a_g \in \mathbb{Z}[G]$. To see that they are the same, write

$$\begin{aligned}\sum_{g,h} n_{g,h}(g,h) &= \sum_{g,h} n_{g,h} g(1, g^{-1}h) \\ &= \sum_{g,k} n_{g,gk} g(1,k) \\ &= \sum_{k} \left(\sum_{g} n_{g,gk} g \right)(1,k) \\ &= \sum_{k} a_k(1,k),\end{aligned}$$

where $k = g^{-1}h$. The reason why the representation $\sum n_{g,h}(g,h)$ is useful is because it's easy to see how the differential d acts on this. The differential is $\mathbb{Z}$-linear map, and it takes the basis element (g,h) to the basis element $(h) - (g)$. The reason why the representation $\sum a_g(1,g)$ is useful is because it's easy to see how an $\mathbb{Z}[G]$-linear map φ acts on it; we just apply φ to the basis elements $(1,g)$ and extend it linearly.

Part III
Applications

5 Hilbert's Theorem 90

Suppose L/K is a cyclic extension with Galois group G and σ a generator of G. We want to show that $H^1(G, L^\times) = 1$. Suppose α is a 1-cocycle. Choose an $x \in L$ such that the set $\{\sigma^i(x) \mid \sigma^i \in G\}$ consists of a normal basis for L. Define a to be

$$a = x + \alpha_\sigma \sigma(x) + \cdots + \alpha_{\sigma^{n-1}} \sigma^{n-1}(x)$$

Since $\alpha_\sigma \neq 0$, we must have $a \neq 0$. We claim that $\alpha = da$. Since α and da are completely determined by their value at σ, it is enough to show that $\alpha_\sigma \sigma(a) = a$:

$$\begin{aligned}\alpha_\sigma \sigma(a) &= \alpha_\sigma \sigma(x) + \alpha_{\sigma^2} \sigma^2(x) + \cdots + \alpha_{\sigma^n} \sigma^n(x) \\ &= \alpha_\sigma \sigma(x) + \alpha_{\sigma^2} \sigma^2(x) + \cdots + x \\ &= a\end{aligned}$$

And we are done.

Example 5.1. Let L/K be the quadratic extension $\mathbb{Q}(i)/\mathbb{Q}$. The Galois group is cyclic of order 2, its generator s acting via conjugation:

$$s: \ c - di \mapsto c + di \ .$$

An element $x = a + bi$ in L has norm $(s \cdot x) = a^2 + b^2$. An element of norm one corresponds to a rational solution of the equation $a^2 + b^2 = 1$ or in other words, a point with rational coordinates on the unit circle. Hilbert's Theorem 90 then states that every element y of norm one can be parametrized (with integral c, d) as
$y = \dfrac{c+di}{c-di} = \dfrac{c^2-d^2}{c^2+d^2} + \dfrac{2cd}{c^2+d^2} i$ which may be viewed as a rational parametrization of the rational points on the unit circle. Rational points $(x,y) = (a/c, b/c)$ on the unit circle $x^2 + y^2 = 1$correspond to Pythagorean triples, i.e. triples (a,b,c) of integers satisfying $a^2 + b^2 = c^2$.

6 Quaternion Algebras

In this section, K will denote a field of characteristic not 2.

Definition 6.1. For any two elements $a, b \in K^\times$ define the **quaternion algebra** $(a,b) = (a,b)_K$ over K as the 4-dimensional K-algebra with a basis $\{1, \alpha, \beta, \alpha\beta\}$ and multipication given by

$$\begin{aligned}\alpha^2 &= a\\ \beta^2 &= b\\ \alpha\beta &= -\beta\alpha\end{aligned}$$

One calls the set $\{1, \alpha, \beta, \alpha\beta\}$ a **quaternion basis** of (a,b).

Let $C = \left(\begin{smallmatrix} c_{11} & c_{12} \\ c_{21} & c_{22}\end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ and set $\alpha' = c_{11}\alpha + c_{12}\beta$ and $\beta' = c_{21}\alpha + c_{22}\beta$. Note that

$$\begin{aligned}\alpha'^2 &= c_{11}^2 a + c_{12}^2 b := a'\\ \beta'^2 &= c_{21}^2 a + c_{22}^2 b := b'\\ \alpha'\beta' &= c_{11}c_{21}a + (\det C)\alpha\beta + c_{12}c_{22}b\\ \beta'\alpha' &= c_{11}c_{21}a - (\det C)\alpha\beta + c_{12}c_{22}b\\ \alpha'\beta' + \beta'\alpha' &= 2(c_{11}c_{21}a + c_{12}c_{22}b).\end{aligned}$$

Thus, in order for $\{1, \alpha', \beta', \alpha'\beta'\}$ to be a quaternion basis, we need $a' \neq 0 \neq b'$ and $c_{11}c_{21}a = -c_{12}c_{22}b$. Assuming these conditions hold, then $\{1, \alpha', \beta', \alpha'\beta'\}$ is a quaternion basis for the quaternion algebra (a', b') and in this case we clearly have $(a,b) \cong (a', b')$. For instance, if $C = \left(\begin{smallmatrix} u & 0 \\ 0 & v\end{smallmatrix}\right)$, then the conditions are satisfied and thus we have an isomorphism $(a,b) \cong (u^2a, v^2b)$. In other words, the isomorphism class of the quaternion algebra (a,b) depends only on the classes of a and b in $K^\times/K^{\times 2}$ Similarly, if $C = \left(\begin{smallmatrix} 0 & ab \\ ab & 0\end{smallmatrix}\right)$, then the conditions are satisfied and thus we have an isomorphisms

$$(a,b) \cong ((ab)^2 b, (ab)^2 a) \cong (b,a).$$

Definition 6.2. Let $Q = (a,b)_K$ be a quaternion algebra and let $q = x + y\alpha + z\beta + w\alpha\beta$ be an element in Q. The **conjugate** of q is the element

$$\overline{q} = x - y\alpha - z\beta - w\alpha\beta.$$

The map from Q to itself given by $q \mapsto \overline{q}$ is an **anti-automorphism** meaning it is a K-linear isomorphism which satisfies $\overline{q_1 q_2} = \overline{q}_2\overline{q}_1$. Moreover, this map is an involution, meaning $\overline{\overline{q}} = q$. We define the **norm** of q to be the element in K given by

$$\mathrm{N}(q) = q\overline{q} = x^2 - ay^2 - bz^2 + abw.$$

The computation

$$\begin{aligned}\mathrm{N}(q_1q_2) &= q_1q_2\overline{q_1q_2}\\ &= q_1q_2\overline{q}_2\overline{q}_1\\ &= q_1\mathrm{N}(q_2)\overline{q}_1\\ &= q_1\overline{q}_1\mathrm{N}(q_2)\\ &= \mathrm{N}(q_1)\mathrm{N}(q_2)\end{aligned}$$

shows that the norm is a multiplicative function from Q to K and is an example of a nondegenerate quadratic form:

Definition 6.3. A **quadratic form** on a vector space V over a field K is a function $Q : V \to F$ such that

1. $Q(\lambda x) = \lambda^2\varphi(x) \qquad \forall \lambda \in K,\ x \in V$
2. The function $B(v,w) := \frac{1}{2}\left(Q(v+w) - Q(v) - Q(w)\right)$

is bilinear. We call B the bilinear form associated to Q. We shall frequently use the second condition as

$$Q(v+w) = Q(v) + Q(w) + 2B(v,w)$$

In particular, note $B(v,w) = 0$ is equivalent to $Q(v+w) = Q(v) + Q(w)$. A quadratic form is said to be **nondegenerate** if its associated bilinear form is nondegenerate: If $B(v,w) = 0$ for all $w \in V$, then $v = 0$. Equivantely if $B(v,w) = 0$ for all $v \in V$, then $w = 0$.

Remark. This definition is coordinate-free, i.e. does not depend on a choice of basis.

The associated bilinear form B_N for the quadratic form $N : (a,b)_K \mapsto K$ can be written down in matrix format

$$B_N(q,q') = \begin{pmatrix} x' & y' & z' & w' \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -a & 0 & 0 \\ 0 & 0 & -b & 0 \\ 0 & 0 & 0 & ab \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = xx' - ayy' - bzz' + abww'$$

Where $q = x + y\alpha + z\beta + w\alpha\beta$ and $q' = x' + y'\alpha + z'\beta + w'\alpha\beta$. When do we have $N(q+\alpha) = N(q) + N(\alpha)$? Whenever $B_N(q,\alpha) = 0$. This happens when $y = 0$. So for example, $N(\beta + \alpha) = N(\beta) + N(\alpha)$. A more interesting case is when $N((1+\alpha)+q) = N((1+\alpha)) + N(q)$. This happens when $B_N(q,(1+\alpha)) = 0$ which leads to the equation $x = ay$. The nondeneracy of the bilinear form can be seen in the matrix representation. If the matrix is invertible, then the bilinear form is nondegenerate.

Lemma 6.1. *An element q of the quaternion algebra $(a,b)_K$ is invertible if and only if it has a nonzero norm. Hence $(a,b)_K$ is a division algebra if and only if the norm $N : (a,b)_K \mapsto K$ does not vanish outside 0.*

Proof. If q has a nonzero norm, then set the inverse of q to be $\frac{\bar{q}}{N(q)}$. Conversely, if q is invertible, then $\bar{q} = N(q)q^{-1}$. And if $N(q)$ is 0, then $\bar{q}$ must be 0 too, hence $q = 0$.

Remark. Hence if q is invertible, its inverse must be $\frac{\bar{q}}{N(q)}$.

□

One can give an intrinsic definition of the conjugation involution (and hence of the norm) on a quaternion algebra $(a,b)_K$ which does not depend on the choice of basis $(1,\alpha,\beta,\alpha\beta)$. Indeed, call an element q of $(a,b)_K$ a **pure quaternion** if $q^2 \in K$ but $q \notin K$. A straightforward computation shows that a nonzero $q = x + y\alpha + z\beta + w\alpha\beta$ is a pure quaternion if and only if $x = 0$. Hence a general q can be written uniquely as $q = q_1 + q_2$ with $q_1 \in K$ and q_2 pure, and conjugation is given by $\bar{q} = q_1 - q_2$. Moreover, a pure quaternion q satisfies $N(q) = -q^2$.

Example 6.1. Besides the classical Hamilton quaternions, the other basic example of a quaternion algebra is the K-algebra $M_2(K)$ of 2×2 matrices. Indeed, the assignment

$$\alpha \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \beta \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

defines an isomorphism $(1,b) \cong M_2(K)$, because the matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & b \\ -1 & 0 \end{pmatrix}$$

generate $M_2(K)$ as a K-vector space, and they satisfy the relations

$$A^2 = Id, \quad B^2 = bId, \quad IJ = -JI$$

Remark. Note that this is not a division algebra. For example, $N(I + A) = 0$, so $I + A$ is not invertible.

Example 6.2. Suppose $K = \mathbb{F}_7$. The quaternion algebra $(-1,-1)$ over K is not a division algebra. Indeed, $2^2 + 3^2 + 1^2 = 0$ in K, so

$$N(2\alpha + 3\beta + \alpha\beta) = 0$$

Definition 6.4. A quaternion algebra over K is called **split** if it is isomorphic to $M_2(K)$ as a K-algebra.

Proposition 6.1. *For a quaternion algebra $(a,b)_K$ the following statements are equivalent.*

1. *The algebra $(a,b)_K$ is split.*
2. *The algebra $(a,b)_K$ is not a division algebra.*
3. *The norm map $N : (a,b)_K \to K$ has a nontrivial zero.*
4. *The element b is a norm from the field extension $K\left(\sqrt{a}\right)/K$.*

Proof.

- $(1 \implies 2)$: $M_2(K)$ has noninvertible elements.
- $(2 \implies 3)$: We proved this above.

- $(3 \implies 4)$: Suppose $N(x + y\alpha + z\beta + w\alpha\beta) = x^2 - ay^2 - bz^2 + abw^2 = 0$ for $x, y, z, w \in K$, not all 0. A potential solution is given by

$$b = \frac{x^2 - ay^2}{z^2 - aw^2} = N_{K(\sqrt{a})/K}\left(\frac{x + y\sqrt{a}}{z + w\sqrt{a}}\right)$$

  This may not be well defined however as $z, w = 0$. So assume $z, w = 0$. If $y = 0$, then $x = 0$ too, so $y \neq 0$. Then $a = \frac{x^2}{y^2} = \left(\frac{x}{y}\right)^2$. This means $K\left(\sqrt{a}\right) = K$, and the norm map is just the identity.

- $(4 \implies 1)$: Suppose $\sqrt{a} \in K$. Then an isomorphism $(a, b)_K \cong M_2(K(\sqrt{a}))$ is given by

$$\alpha \mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} \quad \beta \mapsto m_b = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

  Otherwise, suppose $\sqrt{a} \notin K$ and $N(\gamma) = b$, where $\gamma = r + s\sqrt{a} \in K(\sqrt{a})$, and let σ be the nontrivial galois element in $Gal(K(\sqrt{a})/K)$ which maps $\sqrt{a}$ to $-\sqrt{a}$. Set m_σ to be the matrix representation of σ on the basis $\{1, \sqrt{a}\}$, i.e. $m_\sigma = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Then an isomorphism $(a, b)_K \cong M_2(K(\sqrt{a}))$ is given by

$$\alpha \mapsto m_a = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} \quad \beta \mapsto m_\sigma m_b = \begin{pmatrix} r & as \\ -s & -r \end{pmatrix}$$

□

Example 6.3.

Theorem 6.2. *Suppose n is an integer and p is an odd prime such that $n \not\equiv \square \mod p$. Then $(n, p)_{\mathbb{Q}}$ is a division algebra.*

Proof. To show $(n, p)_{\mathbb{Q}}$ is a division algebra, it suffices to show that if q is a nonzero element of $(n, p)_{\mathbb{Q}}$, then $N(q)$ must be nonzero. We will prove the contrapositive: if q is an element of $(a, p)_{\mathbb{Q}}$ such that $N(q) = 0$, then q must be 0. Suppose $\{1, \alpha, \beta, \alpha\beta\}$ is a quaternion basis for $(n, p)_{\mathbb{Q}}$ and $q = x + y\alpha + z\beta + w\alpha\beta$, then

$$N(q) = x^2 - ny^2 - pz^2 + npw^2 = 0 \quad \implies \quad x^2 - ny^2 = p(z^2 - nw^2)$$

Multilpying through the last equation by a common denominator of x, y, z, w, we can assume that $x, y, z, w \in \mathbb{Z}$. Then if we reduce mod p,

$$x^2 \equiv ny^2 \mod p$$

Assume $x \not\equiv 0 \mod p$. Then $y \not\equiv 0 \mod p$ and $n \equiv \left(\frac{x}{y}\right)^2 \mod p$, which is a contradiction to the assumption in the statement of the theorem. Thus $x \equiv 0 \mod p$, which implies $y \equiv 0 \mod p$. Write $x = px'$ and $y = py'$. Then

$$x^2 - ny^2 = p(z^2 - nw^2) \quad \implies \quad p(x'^2 - ny'^2) = z^2 - nw^2$$

We conclude that $z = pz'$ and $w = pw'$. Then

$$x'^2 - ny'^2 = p(z'^2 - nw'^2)$$

From this, we conclude that $x' = px''$ and $y' = py''$. Repeating this argument shows that x, y, z, w are divisible by arbitrarily high powers of p, so each x, y, z, w must be 0.

□

6.1 Splitting over a Quadratic Extension

Lemma 6.3. *Suppose L is a finite field extension over K, then*

$$L \otimes_K (a, b)_K \cong (a, b)_L$$

Proof. If $\{1, \alpha, \beta, \alpha\beta\}$ is a quaternion basis for $(a, b)_K$, then $\{1 \otimes 1, 1 \otimes \alpha, 1 \otimes \beta, 1 \otimes \alpha\beta\}$ is a quaternion basis for $(a, b)_L$.

$$(1 \otimes \alpha)^2 = (1 \otimes \alpha)(1 \otimes \alpha) = (1 \otimes a) = a(1 \otimes 1)$$
$$(1 \otimes \beta)^2 = (1 \otimes \beta)(1 \otimes \beta) = (1 \otimes b) = b(1 \otimes 1)$$
$$(1 \otimes \alpha)(1 \otimes \beta) = (1 \otimes \alpha\beta) = -(1 \otimes \beta\alpha) = -(1 \otimes \beta)(1 \otimes \alpha)$$

□

Example 6.4. The quaternion algebra $(-1,-1)_{\mathbb{C}}$ is isomorphic to $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H}$. If $\{1, \alpha, \beta, \alpha\beta\}$ is a quaternion basis for $(-1,-1)_{\mathbb{C}}$, then we get an isomorphism from $(-1,-1)_{\mathbb{C}}$ to $M_2(\mathbb{C})$ via

$$1 \mapsto f_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \alpha \mapsto f_1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \beta \mapsto f_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \alpha\beta \mapsto f_3 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

The standard basis of $M_2(\mathbb{C})$ is given by

$$e_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad e_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad e_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \qquad e_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

A change of basis from $\{f_0, f_1, f_2, f_3\}$ to $\{e_0, e_1, e_2, e_3\}$ is given by

$$\frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ -i & 0 & 0 & i \\ 0 & -1 & 1 & 0 \\ 0 & i & i & 0 \end{pmatrix}$$

So for example, since $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)^2 = 0$, we should have $\frac{1}{2}(-1 \otimes \beta + i \otimes \alpha\beta)^2 = 0$. Let's check:

$$\frac{1}{2}(-1 \otimes \beta + i \otimes \alpha\beta)^2 = \frac{1}{2}(-1 \otimes 1 - i \otimes \alpha + i \otimes \alpha + 1 \otimes 1) = 0$$

Definition 6.5. Suppose A is a K-algebra. The **center** $Z(A)$ is the K-subalgebra consisting of elements $x \in A$ satisfying $xy = yx$ for all $y \in A$. If $K = Z(A)$, we say that A is **central** over K.

Proposition 6.2. *A 4-dimensional central division algebra A over K is isomorphic to a quaternion algebra.*

We first need a lemma.

Lemma 6.4. *If A contains a commutative K-subalgebra isomorphic to a nontrivial quadratic field extension $K\left(\sqrt{a}\right)$ of K, then A is isomorphic to a quaternion algebra (a,b) for suitable $a, b \in K^\times$.*

Proof. A K-subalgebra as in the lemma contains an element x such that $x^2 = a$. Since x is not in the center of A, the inner automorphism by $y \mapsto xyx^{-1}$ for $y \in A$ has exact order 2. As a K-linear automorphism of A, it thus has -1 as an eigenvalue, which means that there exists $z \in A$ such that $xzx^{-1} = -z$, or $xz = -zx$. Since z anticommutes with x, the elements $\{1, z\}$ are linearly independent over $K(x)$. This implies that the elements$\{1, x, z, xz\}$ are linearly independent over K: Suppose

$$a_0 + a_1x + a_2z + a_3xz = (a_0 + a_1x) + (a_2 + a_3x)z = 0 \qquad a_i \in K \text{ for } 0 \le i \le 3.$$

Then since the elements $\{1, z\}$ are linearly independent over $K(x)$, we must have $a_0 + a_1x = 0$ and $a_2 + a_3x = 0$. And since the elements$\{1, x\}$ are linearly independent over K, we conclude that $a_i = 0$ for $0 \le i \le 3$. The relation $xz + zx = 0$ then implies that the K-linear automorphism $y \mapsto z^2yz^{-2}$ for $y \in A$, leaves all four basis elements fixed. Thus, z^2 belongs to the center of A, which is K by assumption. The lemma follows by setting $z^2 = b$. □

Now we prove the main proposition

Proof. Let α be an element of $A \setminus K$. Since A is finite dimensional over K, the powers $\{1, \alpha, \alpha^2, \dots\}$ are linearly independent. Thus, there exists a polynomial f with coefficients in K such that $f(\alpha) = 0$. Since A has no zero divisors, we may assume f is irreducible. This means there is a K-algebra homomorphism

$$K[T]/\langle f(T) \rangle \to A$$

which realizes the field $K(\alpha)$ as a K-subalgebra of A. Now the degree $[K(\alpha) : K]$ cannot be 1 as $\alpha \notin K$, and it cannot be 4 as A is not commutative. Hence, $[K(\alpha) : K] = 2$, and the lemma applies. □

Proposition 6.3. *Suppose A is a quaternion algebra over K, and fix an element $a \in K^\times \setminus K^{\times 2}$. The following statements are equivalent.*

1. *A is isomorphic to the quaternion algebra $(a,b)_K$ for some $b \in K^\times$.*
2. *The $K\left(\sqrt{a}\right)$-algebra $K\left(\sqrt{a}\right) \otimes_K A = (a,b)_{K(\sqrt{a})}$ is split.*
3. *A contains a commutative K-subalgebra isomorphic to $K\left(\sqrt{a}\right)$.*

Proof.

- (1) $\implies$ (2) a is a square in $K\left(\sqrt{a}\right)$, so $(a,b) \cong (1,b)$, and the latter algebra is isomorphic to $M_2(K(\sqrt{a}))$.

- (3) $\implies$ (1) one may assume A is nonsplit, in which case Lemma 5.2 applies.
- (2) $\implies$ (3) is easy in the case when $A \cong M_2(K)$: one chooses an isomorphism $M_2(K) \cong (1, a)$ as in Example 5.1 and takes the subfield $K(B)$, where B is the basis element with $B^2 = a$. We now assume A is non-split, and extend the quaternion norm N on A to $A \otimes_K K(\sqrt{a})$ by base change. For $x, y, z, w \in K\left(\sqrt{a}\right)$

$$N(x \otimes 1 + y \otimes \alpha + z \otimes \beta + w \otimes \alpha\beta) = x^2 - ay^2 - bz^2 + abw^2$$

If $x = x_1 + x_2\sqrt{a}$, $y = y_1 + y_2\sqrt{a}$, $z = z_1 + z_2\sqrt{a}$, $w = w_1 + w_2\sqrt{a}$, then we can also write this a

$$\begin{aligned} N(x \otimes 1 + y \otimes \alpha + z \otimes \beta + w \otimes \alpha\beta) &= N(q_1 + q_2\sqrt{a}) \\ &= N(q_0) + N(\sqrt{a}q_1) + 2B_N(q_0, \sqrt{a}q_1) \\ &= N(q_0) + aN(q_1) + 2\sqrt{a}B_N(q_0, q_1) \end{aligned}$$

Where $q_1 = x_1 \otimes 1 + y_1 \otimes \alpha + z_1 \otimes \beta + w_1 \otimes \alpha\beta$ and $q_2 = x_2 \otimes 1 + y_2 \otimes \alpha + z_2 \otimes \beta + w_2 \otimes \alpha\beta$. Since (a, b) is split as a $K\left(\sqrt{a}\right)$-algebra, there exists q_1, q_2, both not 0, such that

$$N(q_1 + q_2\sqrt{a}) = N(q_0) + aN(q_1) + 2\sqrt{a}B_N(q_0, q_1) = 0$$

Now note that since $q_0, q_1 \in A$, the elements $B(q_0, q_1)$ and $N(q_0) + aN(q_1)$ both lie in K. So it follows that

$$\begin{aligned} N(q_0) &= -aN(q_1) \\ 2B(q_0, q_1) &= 0 \end{aligned}$$

Since A is nonsplit, $N(q_0)$ and $N(q_1)$ are not equal to 0. Since $2B(q_0, q_1) = q_0\overline{q}_1 + \overline{q}_0 q_1 = 0$, the element $q_2 = q_0\overline{q}_1 \in A$ satisfies

$$q_2^2 = q_0\overline{q}_1 q_0\overline{q}_1 = -q_0\overline{q}_0 q_1\overline{q}_1 = -N(q_0)N(q_1) = aN(q_1)^2$$

The square of the element $q = q_2 N(q_1)^{-1}$ is then precisely a, so mapping $\sqrt{a}$ to q embeds $K\left(\sqrt{a}\right)$ into A.

□

The crucial ingredient to the proof above, was the existence of a quadratic extension $K\left(\sqrt{a}\right)$. Observe that the algebra $A \otimes_K K\left(\sqrt{a}\right)$ splits over $K\left(\sqrt{a}\right)$, hence it is isomorphic to $M_2\left(K\sqrt{a}\right)$.

$$A \otimes_K K(\sqrt{a}) \cong A \otimes_K K(x)/(x^2 - a) \cong A(x)/(x^2 - a) \cong A(x)/\left(x + \alpha\right) \oplus A(x)/\left(x - \alpha\right)$$

This is analagous to the fact that a finite separable field extension L over K becomes isomorphic to $\bar{K}^{[L:K]}$ when we tensor it with $\bar{K}$. For example

$$\bar{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}(i) \cong \bar{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}(x)/(x^2 + 1) \cong \bar{\mathbb{Q}}(x)/(x^2 + 1) \cong \bar{\mathbb{Q}}(x)/\left(x + i\right) \oplus \bar{\mathbb{Q}}(x)/\left(x - i\right)$$

Here's a more complicated example.

$$\mathbb{Q}(\zeta_8) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}(\zeta_8) \otimes_{\mathbb{Q}} \mathbb{Q}(x)/(x^4 - 2) \cong \mathbb{Q}(\zeta_8)(x)/(x^4 - 2) \cong \mathbb{Q}(\zeta_8)(x)/\left(x^2 + \zeta_8 + \zeta_8^{-1}\right) \oplus \mathbb{Q}(\zeta_8)(x)/\left(x^2 - \zeta_8 - \zeta_8^{-1}\right) \cong \mathbb{Q}(\zeta_8, \sqrt[4]{2}) \oplus \mathbb{Q}(\zeta_8, \sqrt[4]{2})$$

6.2 The associated conic

We now introduce another important invariant of a quaternion algebra $Q = (a, b)_K$, the **associated conic** $C = C(a, b)/K$. By definition, this is the projective plane curve defined by the homogeneous equation

$$ax^2 + by^2 - abz^2 = 0$$

where x, y, z are the homogeneous coordinates in the projective plane $\mathbb{P}^2_K$. Notice, that the points of this curve correspond to the set of all pure quaternions which square to 0. Indeed, if we fix a basis $\{1, \alpha, \beta, \alpha\beta\}$, then we want to get a map which sends the pure quaternion $q = x\alpha + y\beta + z\alpha\beta \in Q$ to the point $[x : y : z] \in C$. We need to be careful though, because there isn't any such map that happens to be well-defined. To get a well-defined map, we need to identity the quaternion q with λq, where $\lambda \in K^\times$. This means we need to pass to projective space. We also want to only consider the pure projective quaternions which square to 0. So keeping these things in mind, we have a way to associate a quaternion $q \in (a, b)_K$ with a point $[x : y : z] \in C$. Of course The projective plane curve C defined by the homogenous equation $ax^2 + by^2 - abz^2 = 0$ is isomorphic an isomorphic to the projective plane curve C' defined by the homogeneous equation $ax^2 + by^2 - z^2 = 0$. Indeed, the substitution $x \mapsto by$, $y \mapsto ax$, $z \mapsto abz$ maps the points $(x, y, z) \in C$ to the points $(by, ax, abz) = (x', y', z') \in C'$, and the substitution $x' \mapsto y/a$, $y' \to x/b$, $z' \mapsto z/ab$ gives an inverse map. On the other hand, there is an

isomorphism from the quaternion algebra $(a,b)_K$ to the quaternion algebra $(1/b,1/a)_K$, given by $\alpha \mapsto \beta/b = \alpha'$ and $\beta \mapsto \alpha/a = \beta'$, and the pure quaternion $q' = x\alpha' + y\beta' + z\alpha'\beta'$ will square to $\frac{1}{ab}(ax^2 + by^2 - z^2)$, and this will be equal to 0 if and only if $ax^2 + by^2 - z^2 = 0$. Which point does q' correspond to in C? We need to reexpress q' in terms of the original basis, $q' = x'\alpha + y'\beta + z'\alpha\beta = \frac{y}{a}\alpha + \frac{x}{b}\beta + \frac{z}{ab}\alpha\beta$. Thus, it corresponds to $[\frac{y}{a} : \frac{x}{b} : \frac{z}{ab}] \in C$. Suppose the two quaternion algebras $(a,b)_K$ and $(c,d)_K$ are isomorphic as K-algebras. This means we have a change of basis from $\{1,\alpha,\beta,\alpha\beta\}$ to $\{1,\alpha',\beta',\alpha'\beta'\}$, where $\alpha'^2 = c$ and $\beta'^2 = d$. The change of basis matrix should look like this

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & f & g & h \\ 0 & k & l & m \\ 0 & n & o & p \end{pmatrix} \qquad f,g,h,k,l,m,n,o,p \in K \quad \det M \neq 0$$

Then the pure quaternion $q = x\alpha + y\beta + z\alpha\beta$ gets mapped to $q' = x\alpha' + y\beta' + z\alpha'\beta' = (fx + gy + hz)\alpha + (hx + ly + mz)\beta + (nx + oy + pz)\alpha\beta = x'\alpha + y'\beta + z'\alpha\beta$. Now the square of q' is just $cx^2 + dy^2 - cdz^2$. What we are saying is that the isomorphism from $(a,b)_K$ to $(c,d)_K$ induces an isomorphism from the projective plane curve C' defined by the homogeneous equation $cx^2 + dy^2 - cdz^2 = 0$ to the projective plane curve C defined by the homogeneous equation $ax^2 + by^2 - abz^2 = 0$.

Proposition 6.4. *The quaternion algebra $Q = (a,b)_K$ is split if and only if the conic $C = C(a,b)/K$ has a K-rational point.*

Proof. If $[x_0,y_0,z_0]$ is a K-ratoinal point in C, then $ax_0^2 + by_0^2 - z_0^2 = 0$. This is the same as saying the pure quaternion $q = \frac{y_0}{a}\alpha + \frac{x_0}{b}\beta + \frac{z_0}{ab}\alpha\beta$ has no inverse, because $\mathrm{N}(q) = \frac{1}{ab}(ax_0^2 + by_0^2 - z_0^2) = 0$. Conversely, if the quaternion algebra is split, then there exists an element $q = x + y\alpha + z\beta + w\alpha\beta \in (a,b)_K$ such that $N(q) = x^2 - ay^2 - bz^2 + abw^2 = 0$, with one of $x,y,z \neq 0$. Then setting $w = 0$ gives us a K-rational point on $C(a,b)/K$.

□

Example 6.5. For $a \neq 1$, the projective conic $ax^2 + (1-a)y^2 = z^2$ has the K-rational point $(1,1,1)$, hence the quaternion algebra $(a,1-a)$ splits by the proposition. This innocent-looking fact is a special case of the so called **Steinberg relation** for symbols that we shall encounter later.

Remark. A well-known fact from algebraic geometry is that a smooth projective conic defined over a field K is isomorphic to the projective line $\mathbb{P}^1_K$ over K if and only if it has a K-rational point. The isomorphism is given by taking the line joining a point P of the conic to some fixed K-rational point O and then taking the intersection of this line with $\mathbb{P}^1_K$ embedded as, say, some coordinate axis in $\mathbb{P}^2_K$.

For example, here's how this works for the circle $x^2 + y^2 = z^2$. First set $z = 1$. We choose O to be the K-rational point $(-1,0)$. Then a line through $(-1,0)$ is of the form $y = m(x+1)$. The point (x,y) is assumed to be on the line and also on the circle, so we get the relations

$$x^2 + y^2 = 1 \quad \text{and} \quad y = m(x+1)$$

These imply $m^2(1+x)^2 = (1-x)(1+x)$, or $(1+x)m^2 = 1-x$. Solving this for x in terms of m, and using the relation $y = m(1+x)$, we obtain

$$x = \frac{1-m^2}{1+m^2} \qquad y = \frac{2m}{1+m^2}$$

Example 6.6. To say a^2, b^2, c^2, and d^2 are in arithmetic progression means $b^2 - a^2 = c^2 - b^2$ and $b^2 - c^2 = d^2 - c^2$. Write these two conditions as

$$a^2 - 2b^2 + c^2 = 0 \qquad b^2 - 2c^2 + d^2 = 0$$

Each equation above cuts out a surface in $\mathbb{P}^3_K$. The eight points $[\pm 1, \pm 1, \pm 1, 1]$ lie on both surfaces. Finding common solutions to both equations means looking at the intersection of the two surfaces, which will be a curve. Call it C. To find an equation for C, we will project C into the projective plane $\{[a,b,c,0]\}$ and work in this plane. We need to make sure our projection is one-to-one on C so no information is lost. If we project C to the plane $\{[a,b,c,0]\}$ in the simple minded way by $[a,b,c,d] \mapsto [a,b,c,0]$, this will be two-to-one on C since $[a,b,c,\pm d]$ will both go to the same point. Set

$$P := [1,1,1,1] \qquad \Pi := \{[a,b,c,0]\} \subset \mathbb{P}^3_K$$

Let $f : \mathbb{P}^3_K \setminus P \to \Pi$ by $f(Q) = \overline{PQ} \cap \Pi$. So $f(Q)$ is the point on the line $\overline{PQ}$ that lies in the plane Π. To find an explicit formula for $f(Q)$, write $Q = [a,b,c,d]$. The line $\overline{PQ}$ is

$$\overline{PQ} = \{\lambda P + \mu Q = [\lambda + \mu a, \lambda + \mu b, \lambda + \mu c, \lambda + \mu d] \mid [\lambda : \mu] \in \mathbb{P}^1_K\}$$

This line meets Π when $\lambda + \mu d = 0$, so $\lambda = -\mu d$. Thus

$$f(Q) = [\mu(a-d), \mu(b-d), \mu(c-d), 0] = [a-d, b-d, c-d, 0]$$

Q	$f(Q)$
$[1,1,1,1]$	$[3,2,1,0]$
$[-1,1,1,1]$	$[1,0,0,0]$
$[1,-1,1,1]$	$[0,1,0,0]$
$[1,1,-1,1]$	$[0,0,1,0]$
$[-1,-1,1,1]$	$[1,1,0,0]$
$[1,-1,-1,1]$	$[0,1,1,0]$
$[-1,1,-1,1]$	$[1,0,1,0]$
$[-1,-1,-1,1]$	$[1,1,1,0]$

Table 1:

We are interested in f not on all $\mathbb{P}^3_K \setminus P$, but specifically on C, which includes P too. What should $f(P)$ mean? We take the tangent line to the curve C at P. The tangent line to the curve C at P is given by the intersection of these two lines

$$2(a-1)-4(b-1)+2(c-1)=0 \qquad 2(b-1)-4(c-1)+2(d-1)=0$$

This line meets Π where $-2a+3b=0$, so the intersection point is $[a,(2/3)a,(1/3)a,0]=[3,2,1,0]$. Thus we define $f: C \to \Pi$ by

$$f([a,b,c,d]) = \begin{cases} [a-d,b-d,c-d,0 & \text{if } [a,b,c,d] \neq [1,1,1,1] \\ [3,2,1,0] & \text{if } [a,b,c,d]=[1,1,1,1] \end{cases}$$

Table 1 gives the projection to Π of the 8 obvious rational points on C.

Remark. The formula for f is not discontinuous at P. Indeed, let's pick a sequence of points on C tending to P and see their f-values tend to $[3,2,1,0]$. For any ϵ let P_ϵ be a point on C with coordinates $d=1$ and $c=1+\epsilon$. The coordinates a and b are determined (up to sign) as

$$P_\epsilon = \left[\sqrt{1+6\epsilon+3\epsilon^2}, \sqrt{1+4\epsilon+2\epsilon^2}, 1+\epsilon, 1\right]$$

Then $P_0 = P$ and for $\epsilon \neq 0$,

$$f(P_\epsilon) = \left[\sqrt{1+6\epsilon+3\epsilon^2}-1, \sqrt{1+4\epsilon+2\epsilon^2}-1, \epsilon, 0\right]$$

To undertstand the behavior of $f(P_\epsilon)$ as $\epsilon \to 0$ (the limit is not $[0,0,0,0]$!), scale the third coordinate to 1

$$f(P_\epsilon) = \left[\frac{\sqrt{1+6\epsilon+3\epsilon^2}-1}{\epsilon}, \frac{\sqrt{1+4\epsilon+2\epsilon^2}-1}{\epsilon}, 1, 0\right]$$

Letting $\epsilon \to 0$, a derivative calculation shows the limit is $[3,2,1,0]$. We want to find an equation for $f(C)$ in the plane Π. Consider the formula for f away from P, when $[a,b,c,d] \neq [1,1,1,1]$, set

$$u=a-d \qquad v=b-d \qquad w=c-d$$

Using the equations of the curve

$$(u+d)^2+(w+d)^2=2(v+d)^2 \qquad (v+d)^2+d^2=2(v+d)^2$$

Expanding the squares and collecting liek terms

Example 6.7. Suppose K is a finite field with q elements. Then any quaternion algebra $(a,b)_K$ is split. To see this, we just need to show that the conic $C(a,b)/K$ has a K-rational point. We shall find a point $(x_0,y_0,1)$. Set $z=1$ and rewrite the equation that defines our conic as

$$ax^2 = 1-by^2$$

As the the multiplicative group $K^\times$ is cyclic of order $q-1$, there are exactly $1+(q-1)/2$ squares in K, including 0. So the sets $\{ax^2 \mid x \in K\}$ and $\{1-by^2 \mid y \in K\}$ have cardinality $1+(q-1)/2$. Suppose they were disjoint from one another. Then K would have $2(1+(q-1)/2)=q+1$ elements, which is a contradiction. Thus, the two sets must intersect, which means $C(a,b)/K$ has a K-rational point.

Example 6.8. Suppose $K = \mathbb{F}_5$. The example above tells us that $(2,3)_K$ is split. Let's explicitily find an isomorphism $(2,3)_K \cong M_2(K)$. Since 2 is not a square, we can construct this isomorphism by finding an element in $K(\sqrt{2})$ with norm 3:

$$N_{K(\sqrt{2})/K}(x + y\sqrt{2}) = x^2 - 2y^2 = 3$$

A solution is given by $x = 1$, $y = 2$. So the isomorphism is given by

$$\alpha \mapsto \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \quad \beta \mapsto \begin{pmatrix} 1 & 4 \\ -2 & -1 \end{pmatrix}$$

Recall that the function field of an algebraic curve C/K is the field $K(C)$ of rational functions defined over some Zariski open subset of C/K. In the concrete case of a conic $C(a,b)/K$, the simplest way to define it is to take the fraction field of the integral domain $K[x,y]/(ax^2 + by^2 - 1)$ which is $K(C(a,b)) = K(x, \sqrt{b - abx^2})$. A crucial observation is the following: The quaternion algebra $(a,b)_K \otimes_K K(C(a,b)) \cong (a,b)_{K(C(a,b))}$ is always split over $K(C(a,b))$. Indeed, the conic $C(a,b)$ always has point over this field, namely $(x,y,1)$. This point is called the **generic point**.

Lemma 6.5. *If $(a,b)_K$ is a quaternion algebra and $c \in K^\times$ is a norm from the field extension $K(\sqrt{a})/K$, then $(a,b)_K \cong (a,bc)_K$.*

Proof. Since $c = r^2 - as^2$, we can write $c = N(q)$, where $q = r + s\alpha$. Then $\{1, \alpha, q\beta, \alpha q\beta\}$ is a quaternion basis of $(a,b)_K$. Indeed, $q\beta$ is a pure quaternion satisfying

$$(q\beta)^2 = -N(q\beta) = -N(q)N(\beta) = bc$$
$$(q\beta)\alpha = -\alpha(q\beta)$$

A change of basis from $\{1, \alpha, \beta, \alpha\beta\}$ to $\{1, \alpha, q\beta, \alpha q\beta\}$ is given by

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & r & -s \\ 0 & 0 & s & r \end{pmatrix}$$

□

Example 6.9. Suppose $(a,b)_K$ is a quaternion algebra over K. Then $(a,b)_K$ is split over K if and only if $(a,b) \otimes_K K(t)$ is split over $K(t)$. The necessity (only if) is obvious: If $(a,b)_K \cong M_2(K)$, then $(a,b)_K \otimes_K K(t) \cong M_2(k) \otimes_K K(t) \cong M_2(K(t))$. For sufficiency, we assume given a point $(x(t), y(t), z(t))$ of $C(a,b)/K(t)$. As the equation defining $C(a,b)/K(t)$

$$ax(t)^2 + by(t)^2 - z(t)^2 = 0$$

is homogeneous, we may assume after multiplication by a common denominator, that $x(t)$, $y(t)$, $z(t)$ all lie in $K[t]$ and one of them has a nonzero constant term. Then specialization gives a K-point $(x(0), y(0), z(0))$ of $C(a,b)$.

Theorem 6.6. *Suppose $Q_1 = (a_1, b_1)_K$, $Q_2 = (a_2, b_2)_K$ are quaternion algebras. The algebras Q_1 and Q_2 are isomorphic over K if and only if the function fields $K(C(a_1, b_1))$ and $K(C(a_2, b_2))$ are isomorphic over K.*

Remark. It is known from algebraic geometry that two smooth projective curves are isomorphic if and only if their function fields are. Thus the theoerem states that two quaternion algebras are isomorphic if and only if the associated conics are isomorphic as algebraic curves.

Example 6.10. Let's prove this for a specific example, the circle. Suppose $K = \mathbb{R}$, $L = \mathbb{C}$, $Q_1 = (-1,-1)_K$, $Q_2 = (a,b)_K$, $C = C(-1,-1)/K$, and $C' = C(a,b)/K$. We have $Q_1 \otimes_K L \cong M_2(L)$. We assume that the function fields $K(C)$ and $K(C')$ are isomorphic over K. The field $L(C)$ is the function field of the curve C_L obtained by extension of scalars from L. This curve is isomorphic to the rational function field $L(t)$ by

$$x \mapsto \frac{1 - t^2}{1 + t^2} = \frac{(1-t)(1+t)}{(1-it)(1+it)} \qquad y \mapsto \frac{2t}{1 + t^2} = \frac{2t}{(1+it)(1-it)}$$

As $Q_2 \otimes_K L(C') \cong Q_2 \otimes_K L(C) \cong Q_2 \otimes_K L(t)$ is split over $L(C) \cong L(t)$ by assumption, it follows that $Q_2 \otimes_K L$ is split over L. Thus $Q_2 \cong (-1, c)$ for some $c \in K^\times$. It follows that $c = N_{L(C)/K(C)}(f)$ for some $f \in L(C)^\times$.

Tensor products of quaternion algebras

Lemma 6.7. *Given two matrix algebras $M_n(K)$ and $M_m(K)$, we have $M_n(K) \otimes_K M_m(K) \cong M_{nm}(K)$*

Proof. Denote $E_{i,j}$ as the matrix with entry 1 in the i'th row and j'th column and entry 0 everywhere else. $M_n(K) \otimes_K M_m(K)$ has basis given by $\{E_{i,j} \otimes E_{k,l}\}$ where $i, j \in \{1, \dots, n\}$ and $k, l \in \{1, \dots m\}$. An isomorphism as K-vector spaces is given by the map which sends $E_{i,j} \otimes E_{k,l} \mapsto E_{ik,jl}$.

□

Lemma 6.8. *Given elements $a, b, b' \in K^\times$, we have an isomorphism*

$$(a, b) \otimes_K (a, b') \cong (a, bb') \otimes_K \mathrm{M}_2(K)$$

Proof. Let $\{1, \alpha, \beta, \alpha\beta\}$ and $\{1, \alpha', \beta', \alpha'\beta'\}$ be quaternion bases for (a, b) and (a, b') respectively. Consider the K-subspaces of $(a, b) \otimes_K (a, b')$ given by

$$A_1 = K(1 \otimes 1) \oplus K(\alpha \otimes 1) \oplus K(\beta \otimes \beta') \oplus K(\alpha\beta \otimes \beta')$$
$$A_2 = K(1 \otimes 1) \oplus K(1 \otimes \beta') \oplus K(\alpha \otimes \alpha'\beta') \oplus K(-b'(\alpha \otimes \alpha'))$$

They are more than just K-subspaces of $(a, b) \otimes_K (a, b')$; they are K-subalgebras of $(a, b) \otimes_K (a, b')$. As a K-algebra, A_1 is generated by $\{\alpha \otimes 1, \beta \otimes \beta'\}$ and A_2 is generated by $\{1 \otimes \beta', \alpha \otimes \alpha'\beta'\}$. By squaring these basis elements, we see that A_1 and A_2 are isomorphic to the quaternion algebras (a, bb') and $(b', -a^2b')$, respectively. The latter algebra is isomorphic to $(b', -b')$, which is split because the conic $C(b', -b')$ has the K-rational point $(1, 1, 0)$. Now consider the map $\rho\colon A_1 \otimes A_2 \to (a, b) \otimes_K (a, b')$ induced by the K-bilinear map $(x, y) \mapsto xy$. Inspection shows that all standard basis elements of $(a, b) \otimes_K (a, b')$ lie in the image of ρ, for example

$$(a^{-1}\alpha\beta \otimes \beta') \otimes (\alpha \otimes b^{-1}\alpha'\beta') \mapsto \beta \otimes \alpha'$$

$$(a^{-1}\alpha \otimes 1) \otimes (\alpha \otimes \alpha'\beta') \mapsto 1 \otimes \alpha'\beta'$$

So ρ is surjective and hence induces an isomorphism as K-vector spaces for dimension reasons. We only need to check that this map ρ respects multiplication, and hence is a K-algebra isomorphism. For that, we simply need to check that A_1 and A_2 commute with each other:

$$(\alpha \otimes 1)(1 \otimes \beta') = (1 \otimes \beta')(\alpha \otimes 1) \qquad (\alpha \otimes 1)(\alpha \otimes \alpha'\beta') = (\alpha \otimes \alpha'\beta')(\alpha \otimes 1)$$
$$(\beta \otimes \beta')(1 \otimes \beta') = (1 \otimes \beta')(\beta \otimes \beta') \qquad (\beta \otimes \beta')(\alpha \otimes \alpha'\beta') = (\alpha \otimes \alpha'\beta')(\beta \otimes \beta')$$

□

Corollary. *For a quaternion algebra (a, b) the tensor product algebra $(a, b) \otimes_K (a, b)$ is isomorphic to the matrix algebra $\mathrm{M}_4(K)$.*

Proof. We have

$$\begin{aligned}(a, b) \otimes_K (a, b) &\cong (a, b^2) \otimes_K \mathrm{M}_2(K) \\ &\cong \mathrm{M}_2(K) \otimes_K \mathrm{M}_2(K) \\ &\cong \mathrm{M}_4(K).\end{aligned}$$

□

Definition 6.6. A **biquaternion algebra** is a K-algebra which is isomorphic to a tensor product of two quaternion algebras over K.

A biquaternion algebra $A = Q_1 \otimes_K Q_2$ is equipped with an involution σ defined as the product of the conjugation involutions on Q_1 and Q_2, i.e. by setting $\sigma(q_1 \otimes q_2) = \overline{q}_1 \otimes \overline{q}_2$ and extending by linearity. This involution is not canonical but depends on the decomposition $A \cong Q_1 \otimes_K Q_2$. For $i = 1, 2$ denote by Q_i^- the subspace of pure quaternions in Q_i.

Lemma 6.9. *Let V be the K-subspace of A consisting of elements satisfying $\sigma(a) = -a$, and W the subspace of those with $\sigma(a) = a$. One has a direct sum decomposition $A = V \oplus W$, and moreover one may write*

$$V = (Q_1^- \otimes_K K) \oplus (K \otimes_K Q_2^-) \qquad \textit{and} \qquad W = K \oplus (Q_1^- \otimes_K Q_2^-)$$

Proof. If we choose quaternion bases $\{1, \alpha_1, \beta_1, \alpha_1, \beta_1\}$ and $\{1, \alpha_2, \beta_2, \alpha_2\beta_2\}$ for Q_1 and Q_2 respectively, then V has as K-basis given by

$$\{1 \otimes \alpha_2, 1 \otimes \beta_2, 1 \otimes \alpha_2\beta_2, \alpha_1 \otimes 1, \beta_1 \otimes 1, \alpha_1\beta_1 \otimes 1\}$$

and W has K-basis given by

$$\{1 \otimes 1, \alpha_1 \otimes \alpha_2, \alpha_1 \otimes \beta_2, \alpha_1 \otimes \alpha_2\beta_2, \beta_1 \otimes \alpha_2, \beta_1 \otimes \beta_2, \beta_1 \otimes \alpha_2\beta_2, \alpha_1\beta_1 \otimes \alpha_2, \alpha_1\beta_1 \otimes \beta_2, \alpha_1\beta_1 \otimes \alpha_2\beta_2\}$$

One has $V \cap W = 0$. Moreover, there are natural inclusions

$$(Q_1^- \otimes_K K) \oplus (K \otimes_K Q_2^-) \subset V \qquad \text{and} \qquad K \oplus (Q_1^- \otimes_K Q_2^-) \subset W$$

For dimension reasons these must be isomorphisms and $V \oplus W$ must be the whole of A. □

Denote by N_1 and N_2 the quaternion norms on Q_1 and Q_2 respetively, and consider the quadratic form

$$\phi(x, y) = N_1(x) - N_2(y)$$

on V, called an **Albert form** of A. Again, it depends on the decomposition $A \cong Q_1 \otimes Q_2$.

Theorem 6.10. *For a biquaternion algebra $A \cong Q_1 \otimes_K Q_2$ over K, the following statements are equivalent:*

1. *The algebra A is not a division algebra.*
2. *There exists $a, b, b' \in K^\times$ such that $Q_1 \cong (a, b)$ and $Q_2 \cong (a, b')$*
3. *The Albert form has a nontrivial zero on A.*

Central simple algebras and Galois Descent

Definition 6.7. A K-algebra A is called **simple** if it has no two-sided ideal other than 0 and A. It is called **central** if its center equals K.

A division algebra D over K is obviously simple. Inverting the relation $xy = yx$ gives $y^{-1}x^{-1} = x^{-1}y^{-1}$ where $y \in D$ and $x \in Z(D)$ shows that its centre is a field. Hence, D is a central simple algebra over $Z(D)$.

Example 6.11. If D is a division ring over K, then $\mathrm{M}_n(D)$ is simple for all $n \geq 1$. Indeed, to show that it is simple, we need to show that $\langle M \rangle = M_n(D)$ for all $M \in M_n(D) \setminus \{0\}$. Since every matrix in a D-linear combination of the E_{ij}, it suffices to show that $E_{ij} \in \langle M \rangle$ for all $i, j \in \{1, \ldots, n\}$. But in view of the relation $E_{k,i}E_{i,j}E_{j,l} = E_{k,l}$, it is enough to show that $E_{i,j} \in \langle M \rangle$ for some $i, j \in \{1, \ldots, n\}$. Choose i, j so that the entry in the i'th row and j'th column of M is a nonzero element m. Then $m^{-1}E_{ii}ME_{jj} = E_{ij}$, and we are done.

Noting the easy fact that in a matrix ring the centre can only contain scalar multiples of the identity, we get that $M_n(D)$ is a central simple algebra over $Z(D)$.

Theorem 6.11 (Wedderburn)**.** *Let A be a finite dimensional simple algebra over a field K. Then there exists an integer $n \geq 1$ and a division algebra $D \supset K$ so that A is isomorphic to the matrix ring $M_n(D)$. Moreover, the division algebra is uniquely determined up to isomorphism.*

The proof will follow from the next two lemmas. Before stating them, let us recall some basic facts from module theory. First, a nonzero A-module M is called **simple** if it has no A-submodules other than 0 and M.

Example 6.12. Let us describe the simple left modules over $M_n(D)$, where D is a divison algebra. For all $1 \leq r \leq n$, consider the subring $I_r \subset M_n(D)$ given by

$$I_r = M_n(D)E_{1,r} + M_n(D)E_{2,r} + \cdots + M_n(D)E_{n,r} = M_n(D)E_{1,r}$$

In view of the relation

$$\begin{cases} E_{i,j}E_{k,r} = 0 & \text{if } j = k \\ E_{i,j}E_{k,r} = E & \text{else} \end{cases}$$

We see that these are simple left $M_n(D)$-modules. Moreover, we have $M_n(D) = \bigoplus I_r$ and the I_r are all isomorphic as $M_n(D)$-modules. Finally, if M is a simple left $M_n(D)$-module, then for every nonzero $m \in M$, we must have $\{xm \mid x \in M_n(D)\} = M$. So choose a nonzero $m \in M$ and define a map from $M_n(D)$ to M to via $x \mapsto xm$ where $x \in M_n(D)$. Viewing $M_n(D)$ and M as left $M_n(D)$-modules, this map is in fact a surjective left module homorophism. But then the induced map $\bigoplus I_r \to M$ must induce an isomorphism with some I_r. Thus all simple left $M_n(D)$-modules are isomorphic to (say) I_1.

Next, an **endomorphism** of a left A-module M over a ring A is an A-homomorphism $M \to M$; these form a ring $End_A(M)$ where addition is given by the rule $(\phi + \psi)(x) = \phi(x) + \psi(x)$ and multiplication by composition of maps. If A is a K-algebra, then so is $End_A(M)$, for multiplication by an element of K defines an element in the centre of $End_A(M)$: If $\varphi \in End_A(M)$ and $x \in K$, then x acts on φ via $x \cdot \varphi = x\varphi$, and $x\varphi \in End_A(M)$ since $x\varphi(am) = xa\varphi(m) = ax\varphi(m)$. In the case when A is a division algebra, M is free over A, thus choosing a basis of M induces an isomorphism $End_A(M) \cong M_n(A)$, where n is the dimension of M over a A. The module M is equipped with a left module structure over $End_A(M)$ via the rule $\phi \cdot m = \phi(m)$ for $m \in M$ and $\phi \in End_A(M)$.

Lemma 6.12 (Schur)**.** *Let M be a simple module over a K-algebra A. Then* $\mathrm{End}_A(M)$ *is a division algebra.*

Proof. The kernel of a nonzero endomorphism $\varphi\colon M \to M$ is an A-submodule different from M, hence it is 0. Similarly, its image must be the whole of M. Thus it is an isomorphism, which means it has an inverse in $End_A(M)$. □

Now let M be a left A-module with endomorphism ring $D = End_A(M)$. As remarked above, M is naturally a left D-module, hence one may also consider the endomorphism ring $End_D(M)$. One defines a ring homomorphism $\lambda_M : A \to End_D(M)$ by sending $a \in A$ to the endomorphism $m \mapsto am$ where $m \in M$. This is indeed a D-endomorphism, for if $\phi \in D$, one has $\phi \cdot am = \phi(am) = a\phi(m) = a\phi \cdot m$ for all $m \in M$.

Lemma 6.13 (Rieffel)**.** *Let L be a nonzero left ideal in a simple K-algebra A, and put $D = End_A(L)$. Then the map $\lambda_L : A \to End_D(L)$ defined above is an isomorphism.*

Proof. Since $\lambda_L \neq 0$, its kernel is a proper two-sided ideal of A. Since A is simple, this ideal must be 0, so λ_L is injective. For surjectivity, we show first that $\lambda_L(L)$ is a left ideal in $End_D(L)$. Indeed, take $\phi \in End_D(L)$ and $l \in L$. Then $\phi \cdot \lambda_L(l)$ is the map $x \mapsto \phi(lx)$ where $x \in L$. But for all $x \in L$, the map $y \mapsto yx$ is an A-endomorphism of L where $y \in L$. As ϕ is a D-endomorphism, we have $\phi(lx) = \phi(l)x$, and so $\phi \cdot \lambda_L(l) = \lambda_L(\phi(l))$. Now observe that the right ideal LA generated by L is a two-sided ideal, hence $LA = A$. In particular, we have $1 = \sum l_i a_i$ with $l_i \in L$ and $a_i \in A$. Hence for $\phi \in End_D(L)$ we have $\phi = \phi \cdot 1 = \phi\lambda_L(1) = \sum \phi\lambda_L(l_i)\lambda_L(a_i)$. But since $\lambda_L(L)$ is a left ideal, we have here $\phi\lambda_L(l_i) \in \lambda_L(L)$ for all i, and thus $\phi \in \lambda_L(A)$. □

Galois Descent

Definition 6.8. For an L-vector space V, a K-subspace W such that K-basis of W is an L-basis of V is called a K-**form** of V.

Example 6.13. $M_2(\mathbb{R})$ and $\mathbb{H}$ are both $\mathbb{R}$-forms of the $\mathbb{C}$-vector space $M_2(\mathbb{C})$. The standard basis $\mathbb{R}$-basis$\{E_{11}, E_{12}, E_{21}, E_{22}\}$ of $M_2(\mathbb{R})$ is a $\mathbb{C}$-basis of $M_2(\mathbb{C})$, and the $\mathbb{R}$-basis $\{E_{11} + E_{22}, -iE_{11} + iE_{22}, E_{21} - E_{12}, -iE_{21} - iE_{12}\}$ of $\mathbb{H}$ is a $\mathbb{C}$-basis of $M_2(\mathbb{C})$.

7 Group Cohomology

In this section, let G be a group, not necessarily profinite, and let A is an abelian group.

Definition 7.1. An **extension** of G by A is a group E, together with an exact sequence:

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

An extension E' of G by A is said to be **isomorphic** to E if there exists an isomorphism $\varphi : E \to E'$ such that the following diagram is commutative

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

If E is an extension of G by A, a **section** of E is a map $s : G \to E$, such that the composite map $G \to E \to G$ is the identity. If π denotes the projection $E \to G$, this means that $\pi \circ s = id_G$. A section s which is a homomorphism is called a **splitting** of E; if such a section exists, we say E **splits**. If s is a splitting, its image is a subgroup C of E, with $C \cap A = 1$ and $AC = E$. The projection $E \to G$ gives an isomorphism $C \to G$, and C is called a **lifting of** G **in E**. If we identify C with G, then every element of E can be written uniquely as ag with $a \in A$ and $g \in G$. The group E is said to be a **semidirect product** of G and A

Given a G-module A, suppose E is a group extension of G by A, that is, E is a group which contains A as a normal subgroup such that $E/A \cong G$, where the given action of G on A is the same as the natural conjugation action induced by this isomorphism, i.e. for each element $g \in G$, let $e_g \in E$ be a coset representative corresponding to g. Then we have

$$E = \coprod_g Ae_g$$

i.e., every element of E is uniquely of the form ae_g. The action then is

$$g \cdot a = e_g a e_g^{-1}$$

This map is well-defined since A is abelian: We need to show that the action does not depend on the choice of a coset representative, so given another coset representative be_g, write

$$\begin{aligned} g \cdot a &= be_g a (be_g)^{-1} \\ &= be_g a e_g^{-1} b^{-1} \\ &= e_g a e_g^{-1} \end{aligned}$$

This map is an action since A is a normal subgroup in E. Another way of thinking of this action is

$$e_g a = (g \cdot a) e_g$$

Suppose the section mapping g to e_g was actually a group theoretic section, i.e. a set theoretic section that is also a homomorphism. Then we have:

$$e_g e_h = e_{gh}$$

In general, this isn't necessarily true. However, since π is a homomorphism which maps e_g to g and e_h to h, we know that

$$e_g e_h = \alpha_{g,h} e_{gh} \qquad \text{for some } \alpha_{g,h} \in A$$

What can we say about $\alpha_{g,h}$? Well since E is a group, the associativity law tells us that on the one hand, we have

$$e_g e_h e_k = \alpha_{g,h} e_{gh} e_k = \alpha_{g,h} \alpha_{gh,k} e_{ghk}$$

On the other, we have

$$e_g e_h e_k = e_g \alpha_{h,k} e_{hk} = e_g \alpha_{h,k} e_g^{-1} e_g e_{hk} = g \cdot \alpha_{h,k} \alpha_{g,hk} e_{ghk}$$

$$(e_g e_h) e_k = \alpha_{g,h} e_{gh} e_k = \alpha_{g,h} \alpha_{gh,k} e_{ghk}$$

So the associativity law implies that α must satisfy the 2-cocycle condition:

$$g \cdot \alpha_{h,k} \alpha_{g,hk} = \alpha_{g,h} \alpha_{gh,k}$$

Now suppose we choose a differenent section $g \mapsto \beta_g e_g$, then

$$\beta_g e_g \beta_h e_h = \beta_g (g \cdot \beta_h) e_g e_h = \alpha_{g,h} \beta_{gh} e_{gh}$$

In other words,

$$e_g e_h = (d\beta)_{g,h} \alpha_{g,h} e_{gh}$$

Proposition 7.1. *An automorphism $\varphi : E \to E$ which induces the identity on A and on E/A is of the form*

$$ae_g \mapsto a\beta_g e_g$$

where β is a 1-cocycle. It is an inner automorphism if and only if β is a coboundary.

Proof. Since φ induces the identity on on E/A, it must map e_g to $\beta_g e_g$, where $\beta \in A$. Since φ induces the identity on A, we must have

$$\varphi(ae_g) = \varphi(a)\varphi(e_g) = a\beta_g e_g$$

We need to check that α is a 1-cocycle, i.e.

$$\beta_{gh} = \beta_g (g \cdot \beta_h)$$

We compute $\varphi(e_{gh})$ in two ways.

$$\varphi(e_{gh}) = \beta_{gh} e_{gh} = \beta_{gh} \alpha_{g,h} e_g e_h$$

$$\varphi(e_{gh}) = \varphi(\alpha_{g,h} e_g e_h) = \alpha_{g,h} \beta_g e_g \beta_h e_h = \alpha_{g,h} \beta_g (g \cdot \beta_h) e_g e_h$$

And so we have

$$\beta_{gh}\alpha_{g,h} = \alpha_{g,h}\beta_g(g\cdot\beta_h)$$

$$\beta_{gh} = \beta_g(g\cdot\beta_h)$$

Now suppose β_g is a coboundary

$$\beta_g = b(g\cdot b)^{-1}$$

Then

$$\varphi(ae_g) = a\beta_g e_g = ab(g\cdot b)^{-1}e_g = abe_g b^{-1}e_g^{-1}e_g = bae_g b^{-1}$$

□

We said earlier that this action is well defined because A is abelian. If A is not abelian, then the action is well defined only up to conjugation. If we restrict the action to the center of A, $Z(A)$, then we get a well defined action again. When A is abelian, $Z(A) = A$, so we may as well consider cohomology with coefficients in $Z(A)$.

7.1 The existence problem and its obstruction in $H^3(G, Z(A))$

Suppose we have a homomorphism $\psi : G \to \mathrm{Out}(A)$. This means to each $g \in G$, we assign a coset of automorphisms of A:

$$g \mapsto \{s_g(\cdot), as_g(\cdot)a^{-1}\dots\}$$

The fact that s_g is an automorphism of A means $s_g xx' = s_g x s_g x'$ for all $x, x' \in A$. The fact that ψ is a homomorphism means $s_g s_h x = s_{g,h}s_{gh}xs_{g,h}^{-1}$ for some $s_{g,h} \in A$ and for all $x \in A$. Notice what happens if we choose different coset representatives: $bs_g as_h xa^{-1}s_g^{-1}b^{-1} = bs_g as_{g,h}s_{gh}xs_{g,h}^{-1}a^{-1}s_g^{-1}b^{-1}$, so this is well defined with $s_{g,h}$ being replaced with $bs_g as_{g,h}$. The question we ask now is, does there exist an extension E of G by A corresponding to ψ? In other words, can we turn s_g into e_g? What Eilenberg and Mac Lane did is to associate to ψ and element $c(\psi)$ of $H^3(G, Z(A))$ and to prove:

Theorem 7.1. *There exists an extension of G by A corresponding to ψ if and only if $c(\psi) = 0$.*

For every $g, h \in G$, choose $s_{g,h} \in A$ such that $s_{g,h}xs_{g,h}^{-1} = s_g s_h s_{gh}^{-1}x$. We can think of this equations like this: We can switch $s_{g,h}$ and x, where $s_{g,h}$ is to the left of x, at the cost of $s_g s_h s_{gh}^{-1}x$.

$$s_{g,h}x = s_g s_h s_{gh}^{-1}xs_{g,h}$$

Now define a 3-cocycle as follows

$$s_{g,h,k} = s_g s_{h,k}s_{g,hk}s_{gh,k}^{-1}s_{g,h}^{-1}$$

Let's show that $s_{g,h,k}$ is an element of $Z(A)$. We do this by showing the associated conjugation map by $s_{g,h,k}$ is trivial.

$$\begin{aligned}
s_{g,h,k}xs_{g,h,k}^{-1} &= s_g s_{h,k}s_{g,hk}s_{gh,k}^{-1}s_{g,h}^{-1}xs_{g,h}s_{gh,k}s_{g,hk}^{-1}s_g s_{h,k}^{-1}\\
&= s_g s_{h,k}s_{g,hk}s_{gh,k}^{-1}s_{gh}s_h^{-1}s_g^{-1}xs_{gh,k}s_{g,hk}^{-1}s_g s_{h,k}^{-1}\\
&= s_g s_{h,k}s_{g,hk}s_{ghk}s_k^{-1}s_{gh}^{-1}s_{gh}s_h^{-1}s_g^{-1}xs_{g,hk}^{-1}s_g s_{h,k}^{-1}\\
&= s_g s_{h,k}s_{ghk}s_k^{-1}s_{gh}^{-1}s_{gh}s_h^{-1}s_g^{-1}xs_g s_{h,k}^{-1}\\
&= s_g s_{h,k}s_{hk}s_{ghk}^{-1}s_{ghk}s_k^{-1}s_{gh}^{-1}s_{gh}s_h^{-1}s_g^{-1}xs_{h,k}^{-1}\\
&= s_g s_h s_k s_{hk}^{-1}s_{hk}s_{ghk}^{-1}s_{ghk}s_k^{-1}s_{gh}^{-1}s_{gh}s_h^{-1}s_g^{-1}x\\
&= x
\end{aligned}$$

7.2 Examples

Example 7.1. We have $\mathrm{Ext}(\mathbb{Z}_2\times\mathbb{Z}_2, \mathbb{Z}_2) \cong H^2(\mathbb{Z}_2\times\mathbb{Z}_2, \mathbb{Z}_2) \cong \mathbb{Z}_8$.
The quaternion group Q_8 fits in the short exact sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow Q_8 \longrightarrow Q_8/\{\pm 1\} \longrightarrow 1$$

a corresponding 2-cocycle is given by

f_2	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	1	1	1	1
$(1,-1)$	1	-1	1	-1
$(-1,1)$	1	-1	-1	1
$(-1,-1)$	1	1	-1	-1

Suppose

f_1	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$f_1(g)$	1	1	1	-1

Then $f_2 df_1$ would be

$f_2 df_1$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	1	1	1	1
$(1,-1)$	1	-1	-1	1
$(-1,1)$	1	1	-1	-1
$(-1,-1)$	1	-1	1	-1

However, all we did here was switch columns up. The dihedral group D_4 fits in the short exact sequence

$$1 \longrightarrow \langle r^2 \rangle \longrightarrow D_4 \longrightarrow D_4/\langle r^2 \rangle \longrightarrow 1$$

The corresponding 2-cocycle is given by

f_2	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	1	1	1	1
$r=(1,-1)$	1	-1	1	-1
$s=(-1,1)$	1	-1	1	-1
$rs=(-1,-1)$	1	1	1	1

The dihedral group $(\mathbb{Z}/2\mathbb{Z})^2/\mathbb{Z}/2\mathbb{Z}$ fits in the short exact sequence

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow 0$$

The corresponding 2-cocycle is given by

f_2	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	1	1	1	1
$r=(1,-1)$	1	1	1	1
$s=(-1,1)$	1	1	1	1
$rs=(-1,-1)$	1	1	1	1

Example 7.2. The group $H^2(S_n, \{\pm 1\})$ is well-known, with the action of S_n on $\{\pm 1\}$ being necessarily the trivial one. Since the action is trivial, the signature homomorphism $S_n \to \{\pm 1\}$ gives rise to an element $\epsilon_n \in H^1(S_n, \{\pm 1\})$. For example, ϵ_3 looks like:

e	(23)	(12)	(123)	(321)	(13)
1	-1	-1	1	1	-1

Now consider the cup product $\epsilon_n \cup \epsilon_n$ induced by the $\mathbb{Z}$-bilinear map:

$B(\cdot,\cdot)$	1	-1
1	1	1
-1	1	-1

For ϵ_3 the resulting cup product looks like:

$B(a_g, g \cdot a_h)$	e	(23)	(12)	(123)	(321)	(13)
e	1	1	1	1	1	1
(23)	1	-1	-1	1	1	-1
(12)	1	-1	-1	1	1	-1
(123)	1	1	1	1	1	1
(321)	1	1	1	1	1	1
(13)	1	-1	-1	1	1	-1

If $n = 2, 3$, then $H^2(S_n, \{\pm 1\}) \simeq \mathbb{Z}/2\mathbb{Z}$ and it is generated by $\epsilon_n \cup \epsilon_n$. If $n \geq 4$, then $H^2(S_n, \{\pm 1\}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ and it is generated by $\epsilon_n \cup \epsilon_n$ and another class t_n. Here is part of it, which you can be completed as an exercise:

$(t_4)_{g,h}$	e	(12)	(23)	(34)	(123)	$(12)(34)$	$(13)(24)$	$(14)(23)$	...
e	1	1	1	1	1	1	1	1	
(12)	1	1	1	1	1				
(23)	1	1	1	1	1				
(34)	1	-1	1	1	1				
$(12)(34)$	1	-1	-1	1	1	-1	1	1	
$(13)(24)$	1					-1	-1	1	
$(14)(23)$	1					1	-1	-1	
...									

Notice the corresponding extension will have identities like:

$$e_{(12)(34)} = -e_{(34)(12)} \qquad \text{and} \qquad e_{(123)(23)} = -e_{(23)(123)}$$

More formally, the extension corresponding to t_n is denoted by $\tilde{S}_n$. Here is a presentation of this group:

$$\tilde{S}_n = < s_i, z \mid s_i^2 = 1,\ z^2 = 1,\ s_i z = z s_i,\ (s_i s_{i+1})^3 = 1,\ s_i s_j = z s_j s_i \text{ if } |j - i| \geq 2 >$$

Now $(\epsilon_n \cup \epsilon_n)(t_n)$ will correspond to another extension which we denote $2 \cdot S_n^-$. Here is its presentation (why?):

$$2 \cdot S_n^- = < s_i, z \mid s_i^2 = z,\ z^2 = 1,\ s_i z = z s_i,\ (s_i s_{i+1})^3 = z,\ s_i s_j = z s_j s_i \text{ if } |j - i| \geq 2 >$$

Now, if G is a subgroup of S_n, we can construct central extensions of G by $\{\pm 1\}$ using the restriction map

$$\text{Res: } H^2(S_n, \{\pm 1\}) \to H^2(G, \{\pm 1\})$$

In particular, we can define the extension $\tilde{G}$ corresponding to $\text{Res}(t_n)$. It is then easy to see that we have the following commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pm 1 & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \pm 1 & \longrightarrow & \tilde{S}_n & \longrightarrow & S_n & \longrightarrow & 1 \end{array}$$

For example, identify the group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with the subgroup V of S_4 where

$$V = \{(),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

Then $\tilde{G} = Q_8$. Can you see it in the table above?

8 Kummer Sequence

Let k^{sep} be a seperable closure of a field k, and denote G_k to mean $Gal(k^{sep}/k)$. Let $n \geq 1$ be an integer, and assume that the image of n in k is nonzero. Then associated to the exaxt sequence

$$0 \longrightarrow \mu_n \longrightarrow (k^{sep})^* \xrightarrow{n} (k^{sep})^* \longrightarrow 0$$

we have a long exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mu_n \cap k & \longrightarrow & k^* & \xrightarrow{n} & k^* \\ & & & & & & \downarrow \delta \\ & & & & H^1(G_k, \mu_n) & \longrightarrow & H^1(G_k, (k^{sep})^*) = 0 \end{array}$$

9 Carlitz Module

The group $(\mathbb{F}_p[T]/M)^\times$ can be interpreted as the Galois group of an extension of the field $\mathbb{F}_p[T]$ in a manner similar to the group $(\mathbb{Z}/(m))^\times$ being the Galois group of the mth cyclotomic extension $\mathbb{Q}(\mu_m)$ of $\mathbb{Q}$, where μ_m is the group of mth roots of unity.

Definition 9.1. For each $M \in \mathbb{F}_p[T]$, we define the **Carlitz polynomial** $[M](X)$ with coefficients in $\mathbb{F}_p[T]$ as follows, start with the initial conditions

$$[1](X) \coloneqq X \text{ and } [T](X) \coloneqq X^p + TX$$

Then proceed using recursion and linearity to obtain $[M](X)$.

Example 9.1. Let $p = 3$. Let's cacluate $[1 + T + T^2]$. First, use recursion

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \dots \\ T & 1 & 0 & 0 & \dots \\ T^2 & T^3 + T & 1 & 0 & \dots \\ T^3 & T^6 + T^4 + T^2 & T^9 + T^3 + T & 1 & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix} \begin{pmatrix} X \\ X^3 \\ X^9 \\ X^{27} \\ \dots \end{pmatrix} = \begin{pmatrix} [1](X) \\ [T](X) \\ [T^2](X) \\ [T^3](X) \\ \dots \end{pmatrix}$$

Next, use linearity

$$[1 + T + T^2](X) = [1](X) + [T](X) + [T^2](X) = (1 + T + T^2)X + (1 + T + T^3)X^3 + X^9$$

Definition 9.2. Let K be a field extension of $\mathbb{F}_p(T)$. We make the additive group of K into and $\mathbb{F}_p[T]$-module by letting $\mathbb{F}_p(T)$ act on K using Carlitz polynomials: for $M \in \mathbb{F}_p[T]$, and $\alpha \in K$, define

$$M \cdot \alpha \coloneqq [M](\alpha).$$

This is called the **Carlitz action** of $\mathbb{F}_p[T]$ on K.

Remark. There are two ways to make the additive group of K into an $\mathbb{F}_p[T]$-module

1. Ordinary multiplication of $\mathbb{F}_p[T]$ on K
2. Carlitz action of $\mathbb{F}_p[T]$ on K.

To avoid ambiguity, we want to denote K differently when it is an $\mathbb{F}_p[T]$-module in each way. A plain K will mean K as an $\mathbb{F}_p[T]$-module by multiplication, while $C(K)$ will mean K as an $\mathbb{F}_p[T]$-module by the Carlitz action.

Definition 9.3. The **M-torsion** Λ_M of the Carlitz module is

$$\Lambda_M = \{\lambda \in \overline{\mathbb{F}_p(T)} \mid [M](\lambda) = 0\}$$

The **Carlitz torsion** is the union of Λ_M over all nonzero $M \in \mathbb{F}_p[T]$.

Example 9.2. Since $[T](X) = X^p + TX = X(X^{p-1} + T)$,

$$\Lambda_T = \{\lambda \in \overline{\mathbb{F}_p(T)} \mid \lambda^p + T\lambda = 0\} = \{0\} \cup \{\lambda \mid \lambda^{p-1} = -T\}$$

which is analogous to

$$\mu_p = \{z \in \overline{\mathbb{Q}} \mid z^p = 1\} = \{1\} \cup \{z \in \overline{\mathbb{Q}} \mid \Phi_p(z) = 0\}$$

Example 9.3. Since $[T^2](X) = (X^p + TX)^p + T(X^p + TX)$,

$$\Lambda_{T^2} = \{\lambda \in \overline{\mathbb{F}_p(T)} \mid \lambda^p + T\lambda \in \Lambda_T\} = \Lambda_T \cup \{\lambda \in \overline{\mathbb{F}_p(T)} \mid (\lambda^p + T\lambda)^{p-1} = -T\}$$

which is analogous to

$$\mu_{p^2} = \{z \in \overline{\mathbb{Q}} \mid z^p \in \mu_p\} = \mu_p \cup \{z \in \overline{\mathbb{Q}} \mid \Phi_p(z^p) = 0\}$$

If $\beta \in \Lambda_{T^2} - \Lambda_T$, then β is a root of $(X^p + TX)^{p-1} + T$, which is irreducible over $\mathbb{F}_p(T)$ since it is Eisenstein with respect to T, so $[\mathbb{F}_p(T, \beta) : \mathbb{F}_p(T)] = p(p-1)$. Moreover, $\alpha \coloneqq [T](\beta) = \beta^p + T\beta$ is a nonzero element of Λ_T and $\Lambda_{T^2} = \{a\alpha + b\beta \mid a, b \in \mathbb{F}_p\}$. So $\mathbb{F}_p(T, \Lambda_T) = \mathbb{F}_p(T, \alpha)$, $\mathbb{F}_p(T, \Lambda_{T^2}) = \mathbb{F}_p(T, \beta)$, and $\mathbb{F}_p(T, \beta)/\mathbb{F}_p(T)$ is a Galois extension. What does the Galois group look like? All elements of $\Lambda_{T^2} - \Lambda_T$ have the same minimal polynomial

$$(X^p + TX)^{p-1} + T$$

and $a\alpha + b\beta \notin \Lambda_T$ when $b \neq 0$, so the $\mathbb{F}_p(T)$-conjugates of β are all $a\alpha + b\beta$ with $a \in \mathbb{F}_p$ and $b \in \mathbb{F}_p^\times$. The $\mathbb{F}_p(T)$-conjugates of β can be written as

$$a\alpha + b\beta = a(\beta^p + T\beta) + b\beta = [aT + b](\beta)$$

where $a \in \mathbb{F}_p$ and $b \in \mathbb{F}_p^\times$. Then $Gal(\mathbb{F}_p(T, \Lambda_{T^2})/\mathbb{F}_p(T)) \simeq (\mathbb{F}_p[T]/(T^2))^\times$ by $\sigma \mapsto aT + b \bmod T^2$, where $\sigma(\beta) = [aT + b](\beta)$.

10 Kummer Sequence

Recall the following short exact sequence

$$0 \longrightarrow \mu_n \longrightarrow (k^{sep})^* \xrightarrow{n} (k^{sep})^* \longrightarrow 0$$

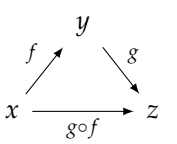
The Carlitz analog of this short exact sequence is this

$$0 \longrightarrow \Lambda_M \longrightarrow \overline{\mathbb{F}_p[T]} \xrightarrow{M} \overline{\mathbb{F}_p[T]} \longrightarrow 0$$

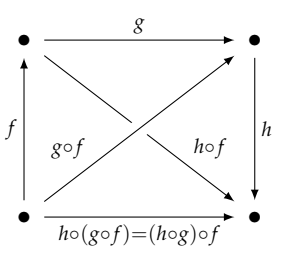
Part IV
Category Theory

A **category C** consists of:

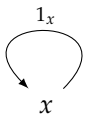
- A class $Ob(\mathbf{C})$ of **objects**. If $x \in Ob(\mathbf{C})$, we simply write $x \in \mathbf{C}$.
- Given $x, y \in \mathbf{C}$, there's a set $Hom_{\mathbf{C}}(x, y)$, called a **homset**, whose elements are called **morphisms** or **arrows** from x to y. If $f \in Hom_{\mathbf{C}}(x, y)$, we write $f : x \to y$.
- Given $f : x \to y$ and $g : y \to z$, there is a morphism called their **composite** $g \circ f : x \to z$.



- Composition is associative: $(h \circ g) \circ f = h \circ (g \circ f)$ if either side is well-defined.



- For any $x \in \mathbf{C}$, there is an **identity morphism** $1_x : x \to x$



- We have the **left and right unity laws**:

$$1_x \circ f = f \text{ for any } f : x' \to x$$

$$g \circ 1_x = g \text{ for any } g : x \to x'$$

Examples of Categories

10.0.1 Categories of mathematical objects

For any kind of mathematical object, there's a category with objects of that kind and morhpisms being the structure-preserving maps between the objects of that kind.

Example 10.1. Sets is the category with sets as objects and functions as morphisms.

Example 10.2. **Sets*** is the category with pointed sets as objects and functions which preserve the base point as morphisms.

Example 10.3. **Grps** is the category with groups as objects and homomorphisms as morphisms.

Example 10.4. **AbGrps** is the category with abelian groups as objects and homomorphisms as morphisms.

Example 10.5. For any field k, $\mathbf{Alg}_k$ is the category with associative unital commutative k-algebras as objects and k-algebra morphisms as morphisms.

Part V
Appendix

Galois Groups

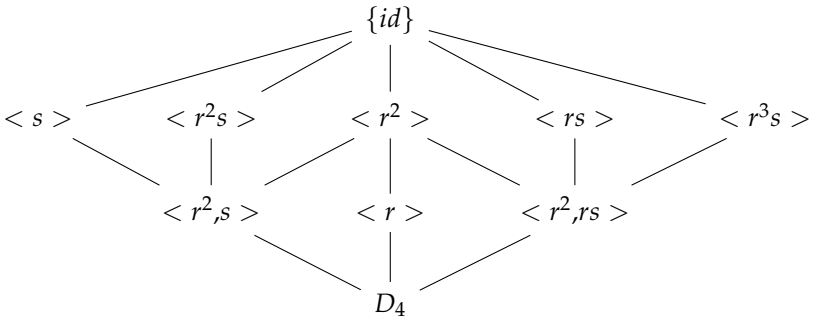
Example 10.6. The extension $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ is Galois since:

1. Any extension of $\mathbb{Q}$ is separable.
2. It is the splitting field over $\mathbb{Q}$ for $x^4 - 2$.

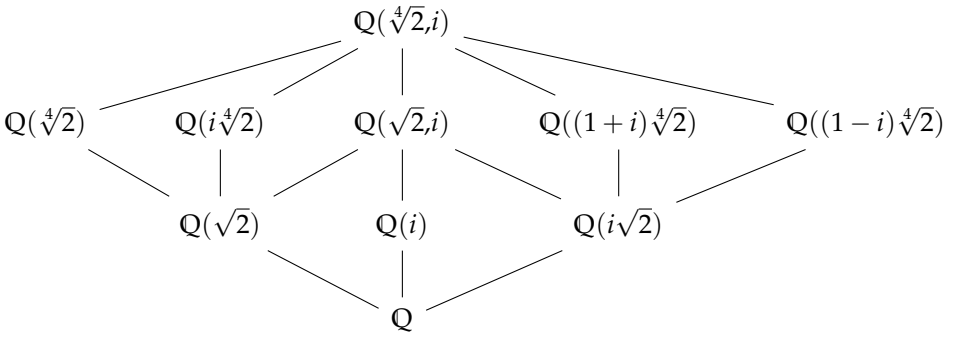
The Galois group for this extension is isomorphic to

$$D_4 =< r, s \mid r^4 = s^2 = 1,\ srs = r^{-1} > .$$

Below is the diagram of all subgroups of D_4, written upside down.



The lattice of intermediate fields in $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ looks the same:



$\mathbb{Q}(i) : \mathbb{Q}$ has degree 2, so its corresponding subgroup H in D_4 has index 2. Since $r(i) = i$, $< r >$ is a subgroup fixing i with index $8/4 = 2$, so $H =< r >$. Thus $Q(i)$ corresponds to $< r >$. The following table shows the 8 different automorphisms of $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$:

σ	id	r	r^2	r^3	s	rs	r^2s	r^3s
$\sigma(\sqrt[4]{2})$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

Infinite Galois Extensions

Definition 10.1. We say that a field extension Ω/k is a Galois extension if it is separable and for every k-linear embedding $\sigma : \Omega \to \bar{k}$ we have $\sigma(\Omega) = \Omega$ (so σ is a k-automorphism of Ω).

Example 10.7. Let $\Omega = \mathbb{Q}(\sqrt{p},\ p\ prime)$ and $G = Gal(\Omega/\mathbb{Q})$. Then $\Omega/\mathbb{Q}$ is a Galois extension with Galois group G. For each prime number p, let σ_p by the unique element of G which maps $\sqrt{p}$ to $-\sqrt{p}$, and fixes everything else. Now consider the subgroup H of $Gal(\Omega/\mathbb{Q})$ generated by the σ_p's. Notice that $H \neq G$ since H does not contain the element $\sigma \in G$ which maps $\sqrt{p}$ to $-\sqrt{p}$ for all prime numbers p. However, we have

$$\Omega^H = \Omega^G = \mathbb{Q}$$

Indeed, any element $x \in \Omega$ is contained in some subfield $E = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})$. Notice that $E/\mathbb{Q}$ is a finite Galois extension. Now assume that $x \in \Omega^H$. Since $\sigma_{p_1}, \ldots, \sigma_{p_k} \in H$, and since they generate $Gal(E/\mathbb{Q})$, we conclude that $x \in \mathbb{Q}$, by classical Galois theory.

In order to get a Galois correspondence, we introduce a topology on G.

Definition 10.2. Let Ω/k be a Galois extension (possibly infinite). The **Krull topology** on Ω/k is the unique topology such that for all $\sigma \in Gal(\Omega/k)$, the family of subsets

$$\{\sigma Gal(\Omega/L) \mid \sigma \in Gal(\Omega/k),\ L/k \text{ is a finite Galois extension, } L \subset \Omega\}$$

is a basis of open neighborhoods of σ. In particular,

$$\{Gal(\Omega/L) \mid\ L/k \text{ is a finite Galois extension, } L \subset \Omega\}$$

is a basis of open neighborhoods of the identity.

Example 10.8. Returning to the previous example, we can easily describe elements in G by a sequence of zeros and ones likeso

$$\sigma_2\sigma_7 = 100100\ldots$$

$$\sigma_{11} = 0000100\ldots$$

$$\sigma_2\sigma_3\sigma_5\cdots = 11111\ldots$$

$$id = 000000\ldots$$

The group operation corresponds to pointwise addition. Open sets are also easy to describe. For example, open neighborhoods of the identity corresponding to this diagram

$$\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}) \hookrightarrow \ldots \hookrightarrow \Omega$$

is

$$G := Gal(\Omega/\mathbb{Q}) \longrightarrow G - \{\sigma_2\} \longrightarrow G - \{\sigma_2, \sigma_3\} \longrightarrow \ldots \longrightarrow \{id\}$$

Example 10.9. The polynomial $x^4 - x^2 - 1$ is irreducible over $\mathbb{Q}$. Let $\alpha = \sqrt{\frac{(1+\sqrt{5})}{2}}$, the four roots of $x^4 - x^2 - 1$ are $\alpha, -\alpha, \frac{i}{\alpha}, \frac{-i}{\alpha}$. Therefore the splitting field of $x^4 - x^2 - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\alpha, i)$.

We have the following examples of fixed subgroups of D_4-modules:

A	A^{D_4}
$(\mathbb{Q}(\sqrt[4]{2}, i), +)$ as an additive group	$\mathbb{Q}^+$
$(\mathbb{Q}(\sqrt[4]{2}, i), \cdot)$ as a multipicative group	$\mathbb{Q}^*$
$(\mathbb{Q}(\sqrt[4]{2}, i)[x,y]/(y^2 - x^3 - 1), +)$	$\mathbb{Q}[x,y]/(y^2 - x^3 - 1)$

The last row is an elliptic curve with it's group structure. First, let's compute $H^*(D_4; \mathbb{Q}(\sqrt[4]{2}, i)^+)$: What is $H^0(D_4; \mathbb{Q}(\sqrt[4]{2}, i)^+)$? To compute this, we look at this sequence:

$$0 \longrightarrow C^0(G, A) \xrightarrow{d} C^1(G, A)$$

Now the image of $0 \to C^0(G, \mathbb{Q}(\sqrt[4]{2}, i))$ is trivial, and the kernel of $d : C^0(G, A) \to C^1(G, A)$ is $\mathbb{Q}(\sqrt[4]{2}, i)^{D_4} = \mathbb{Q}^+$. Therefore $H^0(D_4; \mathbb{Q}(\sqrt[4]{2}, i)^+) = Q^+/0 = Q^+$. Now, what about $H^1(D_4; \mathbb{Q}(\sqrt[4]{2}, i)^+)$? What is in the kernel of $d : C^1(G, \mathbb{Q}(\sqrt[4]{2}, i)) \to C^2(G, \mathbb{Q}(\sqrt[4]{2}, i))$? They must be functions $f_1 : G \to \mathbb{Q}(\sqrt[4]{2})$ such that:

Part VI
Answers

1. No. Even though inverses satisfy the relation $(q_1 q_2)^{-1} = q_1^{-1} q_2^{-1}$, they are not linear. For example, given $i, j \in \mathbb{H}$, the inverse of i is $-i$ and the inverse of j is $-j$, but the inverse of $i + j$ is $\frac{1}{2}(-i - j)$.