

# GALOIS THEORY OF RING SPECTRA

ABSTRACT. If/when you find any errors, send me an email at [brazelton@math.harvard.edu](mailto:brazelton@math.harvard.edu)

## 0. ABOUT

Notes from a talk in the Harvard/MIT BabyTop seminar, April 15th, 2025.

**0.1. References used.** All the classical references (Auslander-Goldman, etc.) were helpful, as was Rognes' paper and Akhil Mathew's papers and notes on the topic. Chapter 6 of Lennart Meier's PhD thesis is a great reference for this subject. I also had some really helpful correspondence with Daniel Davis while prepping this talk, and Liam Keenan and Andy Senger answered some random questions I had throughout.

## 1. DESCENT FOR VINTAGE RINGS

Let  $R \rightarrow S$  be a ring homomorphism. If we think about this as a one-object cover  $\mathrm{Spec}(S) \rightarrow \mathrm{Spec}(R)$ , we can consider its Čech complex, which is an augmented simplicial object

$$\mathrm{Spec}(R) \leftarrow \mathrm{Spec}(S) \rightrightarrows \mathrm{Spec}(S \otimes_R S) \cdots$$

If  $\mathcal{F}: \mathrm{CRing} \rightarrow \mathcal{C}$  is any presheaf valued in any  $\infty$ -category, we can ask whether  $\mathcal{F}$  admits *descent* along this cover, which is the same as saying that the induced map

$$\mathcal{F}(R) \rightarrow \lim(\mathcal{F}(S) \rightrightarrows \mathcal{F}(S \otimes_R S) \cdots)$$

is an equivalence.

If  $\mathcal{F}$  is valued in a 1-category like sets or abelian groups, the limit condition truncates at the second stage, and we recover the sheaf condition. We'll be interested in the case where  $\mathcal{F}(U)$  is a 1-category (and hence lives in a 2-category). Here we get the stack condition.

The particular case we care about is the functor

$$\mathrm{Mod}(-): \mathrm{CRing} \rightarrow \mathrm{Cat},$$

outputting the 1-category of modules over any input ring.

**Theorem 1.1** (Grothendieck). If  $R \rightarrow S$  is a faithfully flat ring extension, then the induced map

$$(1) \quad \mathrm{Mod}_R \rightarrow \lim(\mathrm{Mod}_S \rightrightarrows \mathrm{Mod}_{S \otimes_R S} \cdots)$$

is an equivalence of categories.

This is called *faithfully flat descent*, and it's a shade of a more general result, namely that  $\mathrm{QCoh}$  is an fpqc stack. The category on the right is often called the category of *descent data*.

**Remark 1.2** (On comonadicity). This result about descent can be equivalently phrased in terms of comonadicity. Recall we have an extension-restriction of scalars adjunction

$$-\otimes_R: \text{Mod}_R \rightleftarrows \text{Mod}_S.$$

Then we obtain a comonad  $\Omega$  on  $\text{Mod}_S$ . The category of coalgebras  $\text{coAlg}_\Omega(\text{Mod}_S)$  can be identified with the category of descent data, hence the descent condition can be reframed into a comonadicity condition. This is an important perspective to keep in mind when trying to transport these ideas to spectral algebraic geometry.

We can ask if the theorem above is if and only if – that is, if  $\text{Mod}$  admits descent along a ring extension, then was that extension necessarily faithfully flat? The answer is no!

**Theorem 1.3** ([JT84, pp. 18-19]). Given a commutative ring map  $R \rightarrow S$ , the following are equivalent:

- (1) Equation (1) is an equivalence
- (2) Extension of scalars along  $R \rightarrow S$  is comonadic
- (3)  $S$  is *pure* as an  $R$ -module<sup>1</sup>
- (4) Extension of scalars is faithful.

The latter two come from the fact that a left adjoint is fully faithful if and only if the unit is a componentwise monomorphism.

## 2. GALOIS DESCENT FOR VINTAGE RINGS

A particular case of descent for modules is along *Galois ring extensions*. In this case, the category of descent data admits a nice equivariant description.

**Definition 2.1.** Let  $k \subseteq L$  be a finite field extension. We say it is *Galois* if  $k$  is the fixed field for some subgroup of  $\text{Aut}(L)$ .

We might ask whether we can extend the notion of a Galois field extension to a Galois *ring* extension. This was first done by Auslander and Goldman [AG60], and multiple other equivalent definitions can be found in work of Chase, Harrison and Rosenberg [CHR65].

**Definition 2.2.** Let  $S \in \text{CRing}$ , let  $G \leq \text{Aut}(S)$  be a finite subgroup, and let  $R = S^G$ . We say that  $R \rightarrow S$  is a *Galois ring extension* if the analogue of a normal basis theorem holds, that is if

$$\begin{aligned} S \otimes_R S &\rightarrow \prod_{g \in G} S \\ s_1 \otimes s_2 &\mapsto (s_1 g(s_2))_{g \in G} \end{aligned}$$

is an isomorphism of  $S$ -algebras. Note that this is equivalent to  $R \rightarrow S$  being finite étale in this setting (Proposition A.3, at least when  $S$  is irreducible?).

**Remark 2.3.** There are a ton of equivalent definitions but they imply in particular that  $S$  needs to be finitely generated and projective over  $R$ .

**Example 2.4** ([Rog08b, 2.3.3]). If  $K \subseteq L$  is a  $G$ -Galois extension of number fields, then  $\mathcal{O}_K \rightarrow \mathcal{O}_L$  is a  $G$ -Galois extension of rings if and only if  $K \subseteq L$  is unramified.

**Example 2.5.** There are no nontrivial connected Galois extensions of  $\mathbb{Z}$ .

<sup>1</sup>This means  $R \otimes_R M \rightarrow S \otimes_R M$  is injective for every  $M \in \text{Mod}_R$ . Equivalently the unit of the restriction-extension adjunction is a levelwise monomorphism. The reader is warned not to conflate what Joyal and Tierney call *pure* with what Raynaud and Gruson call *pure* in [RG71, §3.3].

*Proof.* See [Rog08b, 10.3.2]. We know by Minkowski's theorem in algebraic number theory that if  $K$  is any number field, then the map  $\mathbb{Z} \rightarrow \mathcal{O}_K$  ramifies at at least one prime, hence is not étale. So there are no rings of integers which are Galois over  $\mathbb{Z}$ . If  $\mathbb{Z} \rightarrow R$  is  $G$ -Galois for some arbitrary ring  $R$ , then  $R$  is finitely generated and free over  $\mathbb{Z}$  by necessity, hence  $\mathbb{Q} \rightarrow \mathbb{Q} \otimes R$  is a  $G$ -Galois extension, implying  $\mathbb{Q} \otimes R \cong \prod_i K_i$  is a product of number fields. The integral closure of  $R$  is contained in  $\prod \mathcal{O}_{K_i}$ , which implies each  $K_i = \mathbb{Q}$ .  $\square$

**Proposition 2.6** (see [Rog08b, 2.3.4]). If  $R \rightarrow S$  is a  $G$ -Galois extension, then  $S$  is faithfully flat<sup>2</sup> as an  $R$ -module.

### 2.1. A nice characterization of the category of descent data along a Galois extension.

If  $G \leq \text{Aut}(S)$ , then  $G$  acts on the category of  $S$ -modules in a natural way. We can let  $EG$  denote a free contractible  $G$ -category, and define the category of *homotopy fixed points* as

$$\text{Mod}_S^{hG} := \text{Fun}(EG, \text{Mod}_S)^G.$$

**Proposition 2.7.** If  $R \rightarrow S$  is a  $G$ -Galois ring extension, then the category of descent data is equivalent to  $\text{Mod}_S^{hG}$ , and the descent statement can be rephrased as an equivalence of categories

$$\text{Mod}_R \xrightarrow{\sim} \text{Mod}_S^{hG}.$$

**Example 2.8.** In the simple case of  $\mathbb{R} \subseteq \mathbb{C}$ , and  $G = C_2$ , we have that  $C_2$  acts on  $\text{Vect}_{\mathbb{C}}$  by sending each complex vector space to its conjugate. The category  $\text{Mod}_{\mathbb{C}}^{hC_2}$  is then the category of isomorphisms  $V \cong \bar{V}$ .

**Remark 2.9.** If  $\theta: G \rightarrow \text{Aut}(S)$  is our representation, we can define  $S_{\theta}[G]$  to be the *twisted group ring*, with multiplication

$$s_1 g_1 \cdot s_2 g_2 = s_1 \theta_{g_1}(s_2) g_1 g_2.$$

Then we have that

$$\text{Mod}_S^{hG} \cong \text{Mod}_{S_{\theta}[G]}.$$

The twisted group ring is not commutative in general, clearly.

## 3. HOMOTOPICAL GALOIS THEORY

Rognes was the first to try to extend the theory of Galois ring extensions from vintage rings to ring spectra.

**Definition 3.1** (Rognes). Let  $G$  be a finite group and let  $A \rightarrow B$  be a map of  $E_{\infty}$ -rings. We say that it is a  *$G$ -Galois extension* for some finite subgroup  $G \leq \text{Aut}_{\text{CAlg}_A}(B)$  if the induced maps

$$\begin{aligned} A &\rightarrow B^{hG} \\ B \otimes_A B &\rightarrow \prod_{g \in G} B \end{aligned}$$

are equivalences.

Why would we care? In the classical theory of Galois ring extensions, the main goal was to see a nice characterization of  $A$ -modules in terms of homotopy fixed points of the categories of  $B$ -modules, giving us a nice descent condition to check. We want an analogous result here, but we could also ask for some more stuff, for instance: can we compare  $\pi_* A$  and  $\pi_* B$ ?

<sup>2</sup>Recall this means  $S \otimes_R -$  preserves and reflects exact sequences.

The answer to the first is yes, via the *homotopy fixed points spectral sequence*, which in the setting of a  $G$ -Galois extension  $A \rightarrow B$  of  $E_\infty$ -ring spectra takes the form

$$E_2^{p,q} = H^p(G; \pi_q B) \Rightarrow \pi_{q-p} A.$$

In fact the information often flows the other way!

**Proposition 3.2** ([Rog08b, 5.3.1]). The ring extension  $\mathrm{KO} \rightarrow \mathrm{KU}$  is a  $C_2$ -Galois ring extension.

*Proof sketch.* The argument that

$$\mathrm{KO} \rightarrow \mathrm{KU}^{hC_2}$$

is an equivalence dates back to Atiyah, and follows by a spectral sequence argument. You can find this written up really nicely in some [notes of Arun Debray](#).

The argument that  $\mathrm{KU} \otimes_{\mathrm{KO}} \mathrm{KU} \rightarrow \mathrm{KU} \times \mathrm{KU}$  is an equivalence is a bit more involved, leveraging Bott periodicity and nilpotence.  $\square$

**Example 3.3.** The map

$$\mathrm{ko} \rightarrow \mathrm{ku}$$

is not Galois (see [Rog08b, p. 27]).<sup>3</sup>

**Proposition 3.4 (Sanity check [Rog08b, 4.2.1]).** If  $R \rightarrow S$  is a map of vintage commutative rings, and  $G \leq \mathrm{Aut}_{\mathrm{Alg}_R}(S)$ , then  $R \rightarrow S$  is a  $G$ -Galois extension if rings if and only if  $HR \rightarrow HS$  is a  $G$ -Galois extension of ring spectra.

As another sanity check, we can ask whether a Galois extension is dualizable over the base ring. This is true [Rog08b, 6.2.1]. What is not necessarily true, however, is that a Galois extension is faithfully flat.

**3.1. Faithfulness.** We saw for discrete rings that each Galois extension was faithfully flat. We might ask if the same thing is true in higher algebra. The analogue we use here is just *faithfulness*.

**Definition 3.5** ([Rog08b, 4.3.1]). If  $A \in \mathrm{CAlg}(\mathrm{Sp})$ , and  $M \in \mathrm{Mod}(A)$ , we say that  $M$  is *faithful* if, for any  $N \in \mathrm{Mod}_A$ , if  $N \otimes_A M \simeq *$  then  $N \simeq *$ .

**Theorem 3.6.** Let  $f: A \rightarrow B$  be a  $G$ -Galois map of ring spectra, for  $G$  a finite group. Then the following are equivalent:

- (1)  $B$  is faithful (considered as an  $A$ -module)
- (2) Extension of scalars

$$\mathrm{Mod}(A) \rightarrow \mathrm{Mod}(B)$$

is conservative.

- (3) We have descent along  $f$  in the sense that

$$\mathrm{Mod}(A) \xrightarrow{\sim} \mathrm{Mod}(B)^{hG}$$

is an equivalence.

- (4) An analogue of Hilbert 90 holds ([BD10, 1.0.2]):

$$B^{tG} \simeq *$$

---

<sup>3</sup>The fiber of  $\mathrm{ko} \rightarrow \mathrm{ku}^{hC_2}$  is  $\bigotimes_{j < 0} \Sigma^{4j} H\mathbb{Z}/2$ , and the cofiber of  $\mathrm{ku} \otimes_{\mathrm{ko}} \mathrm{ku} \rightarrow \mathrm{ku} \times \mathrm{ku}$  is  $H\mathbb{Z}$  [Rog08b, p. 27].

*Proof.* The equivalence of the first two is clear. The fact that a faithful Galois ring extension satisfies descent can be found in [Ban17, 2.6], in [Mei12, §6], or in [Mat16, 9.4]. Similarly if we have descent, then  $\mathrm{Mod}(A) \rightarrow \mathrm{Mod}(B)^{hG}$  is certainly conservative (being an equivalence of categories), hence  $\mathrm{Mod}(A) \rightarrow \mathrm{Mod}(B)$  is conservative, since the inclusion  $\mathrm{Mod}(B)^{hG} \rightarrow \mathrm{Mod}(B)$  is always conservative. The equivalent definition using the Tate construction is [Rog08b, 6.3.3].  $\square$

It is *not true* that every  $G$ -Galois extension is faithful in homotopical Galois theory – this is a big difference between the homotopical and the classical setting. A counterexample was pointed out by Ben Wieland and can be found in an unpublished note of Rognes [Rog08a]. However an easy example where extensions *are* faithful is the following.

**Example 3.7** ([Rog08b, 6.3.4]). If  $A \rightarrow B$  is a finite  $G$ -Galois extension and  $|G|$  is invertible in  $\pi_0 B$ , then  $A \rightarrow B$  is faithful. This is because the norm map induces an isomorphism on homotopy.

**Remark 3.8.** If  $A \rightarrow B$  is faithful and  $B$  is a dualizable  $A$ -module, then  $A \rightarrow A_B^\wedge$  is an equivalence [Rog08b, 8.2.4].

**Example 3.9.** We have that  $\mathbb{S} \rightarrow \mathrm{MU}$  is not faithful [Rog08b, 12.2.4], despite the fact that  $\mathbb{S} \rightarrow \mathbb{S}_{\mathrm{MU}}^\wedge$  is an equivalence. Rognes invites us to think about the unit map  $\mathbb{S} \rightarrow \mathrm{MU}$  as some massive “near-maximal ramified Galois extension” [Rog08b, p. 6, p. 92].

**Remark 3.10.** There is an analogue of twisted group rings in this setting, constructed as  $G_+ \wedge B$ , with analogous properties to those found in the classical setting [Mei12, 6.1.3, 6.1.4]. It agrees with  $\mathrm{Hom}_A(B, B)$  in the case where  $A \rightarrow B$  is faithful [Mei12, 6.2.4]. The equivalence of module categories above can be proven by translating through the twisted group ring perspective, but in order to argue this way faithfulness is needed.

#### 4. THE PROFINITE GALOIS CORRESPONDENCE

**Theorem 4.1** (Devnatz-Hopkins). There is a weak equivalence

$$L_{K(n)}\mathbb{S} \rightarrow E_n^{h\mathbb{G}_n}.$$

We want to say this is a Galois ring extension, but recall Rognes’ definition requires the group to be finite, whereas the Morava stabilizer group  $\mathbb{G}_n$  is profinite. It is for this reason that Rognes extends his definition to a profinite Galois extension. To talk about this, let’s first double back to the ordinary profinite Galois correspondence.

We know the classical Galois correspondence – between subgroups of some finite Galois group  $G = \mathrm{Gal}(L/k)$  and intermediate Galois field extensions of  $k \subseteq L$ . Grothendieck advocated a more general perspective on this, leveraging the *absolute Galois group*, which we’ll denote by  $G_s = \mathrm{Gal}(k^s/k)$ .

**Theorem 4.2** (Grothendieck Galois correspondence). There is an equivalence of categories

$$\mathrm{FEt}_k^{\mathrm{op}} \xrightarrow{\sim} \mathrm{Fin}_{G_s},$$

between the category of finite étale  $k$ -algebras and finite sets equipped with a continuous  $G_s$ -action.

In particular if  $G$  is a finite group, then a continuous homomorphism  $G_s \rightarrow G$  corresponds to a  $G$ -Galois extension of  $k$ . We can ask whether a similar object exists when  $k$  is a discrete ring, rather than a field, and this is given by the étale fundamental group.

**Theorem 4.3.** For  $R$  a discrete commutative ring, there is an equivalence of categories

$$\mathrm{FEt}_R^{\mathrm{op}} \cong \mathrm{Fin}_{\pi_1^{\mathrm{et}}(R)}.$$

Finally, an analogous question can be asked for ring spectra, and we obtain a profinite Galois correspondence for ring spectra, due to Akhil Mathew. The correct analogue here is something called the *Galois group of an  $E_\infty$ -ring*, which is denoted  $\pi_1(\mathrm{Mod}(R))$  ([Mat16, 6.9]).

**Theorem 4.4** ([Mat16]). If  $R$  is an  $E_\infty$ -ring and  $G$  is any finite group, there is a canonical bijection between continuous homomorphisms  $\pi_1(\mathrm{Mod}(R)) \rightarrow G$  and  $G$ -Galois extensions of  $R$  in the sense of Rognes.

In particular, computing  $\pi_1(\mathrm{Mod}(R))$  lets us understand the Galois theory of the ring spectrum  $R$ . There is always a surjective map

$$\pi_1(\mathrm{Mod}(R)) \twoheadrightarrow \pi_1^{\mathrm{et}}(R_0),$$

where  $R_0 = \pi_0 R$ , but this is in general not an isomorphism. There are nice settings where it is, however.

**Theorem 4.5** ([Mat16, 1.2]). If  $R$  is even periodic and  $\pi_0 R$  is regular and Noetherian, then  $\pi_1(\mathrm{Mod}(R)) \cong \pi_1^{\mathrm{et}}(R)$  – that is, the Galois theory is completely determined by its discrete part.

**Theorem 4.6** ([Mat16, 1.3]). We have that the Galois group of  $K(n)$ -local spectra is the extended Morava stabilizer group.

**Example 4.7.** Every non-trivial ring is faithful over the  $K(n)$ -local sphere in the  $K(n)$ -local setting [Rog08b, 4.3.7].

A quick remark about this — any finite subquotient of the Morava stabilizer group (of which there are many) yields a Galois ring extension of the  $K(n)$ -local sphere, and the methods of Devinatz and Hopkins, combined with these perspectives of Rognes, allow for a study of the  $K(n)$ -local category via Galois theory. The investigation into Galois extensions of the  $T(n)$ -local sphere was one of the motivations for the recent work that led to the disproof of the telescope conjecture.

Another important example is the most basic one, that of the sphere spectrum.

**Theorem 4.8** ([Rog08b, 10.3.3], [Mat16, 6.19]). We have that  $\pi_1(\mathrm{Sp}) = *$  is trivial, i.e. there are no nonseparable Galois extensions of  $\mathbb{S}$ .

We might phrase this as “the sphere spectrum is separably closed” [Rog08b, 1.3]. Let’s prove this, following Rognes.

*Proof sketch.* Suppose that  $\mathbb{S} \rightarrow B$  is some finite  $G$ -Galois extension. Then we can argue  $B$  is dualizable as a module over  $\mathbb{S}$ , hence has the homotopy type of a retract of a finite CW spectrum. This implies its integral homology is finitely generated in each degree, and only nonzero in finitely many degrees. Leveraging the condition  $B \wedge B \cong \prod_{g \in G} B$ , we can argue that the homology must be concentrated in degree zero, implying by Hurewicz that  $B$  is connective, with  $\pi_0 B \cong H_0 B$  some free abelian  $\mathbb{Z}$ -module of rank equal to  $\#G$ , which will turn out to be faithfully flat. We can then use this to argue that  $\mathbb{Z} = \pi_0 \mathbb{S} \rightarrow \pi_0 B$  is a  $G$ -Galois extension of commutative rings, which by the theorem of Minkowski implies that  $\pi_0 B \cong \mathbb{Z}^{\#G}$ . In particular  $B$  is the Moore spectrum  $S\mathbb{Z}^{\#G} = \bigvee_{g \in G} \mathbb{S}$ .  $\square$

## APPENDIX A. GALOIS AND ÉTALE RING EXTENSIONS

Let  $f: R \rightarrow S$  be a map of commutative rings. We always have a natural map

$$\begin{aligned} \mathrm{Hom}_R(S, R) \otimes_R S &\rightarrow \mathrm{End}_R(S) \\ \lambda \otimes s &\mapsto [s' \mapsto \lambda(s')s]. \end{aligned}$$

In the case where  $S$  is finitely generated and projective over  $R$ , this is an isomorphism, whose inverse is of the form  $\mathrm{End}_R(S) \cong S^\vee \otimes_R S$ , where  $(-)^\vee$  denotes the categorical dual in  $\mathrm{Mod}_R$ .

**Definition A.1** (see e.g. [Knu91, 7.3.3]). If  $f$  exhibits  $S$  as a finitely generated projective  $R$ -module, then we can define the *reduced trace*

$$\mathrm{tr}_{S/R}: \mathrm{End}_R(S) \rightarrow R$$

given by the evaluation map  $S^\vee \otimes_R S \rightarrow R$ .

Denote by

$$\begin{aligned} \rho: S &\rightarrow \mathrm{End}_R(S) \\ s &\mapsto \mathrm{mult}_s \end{aligned}$$

the *regular representation* of  $S$  as an  $R$ -algebra.

**Definition A.2.** If  $S$  is a commutative  $R$ -algebra which is finitely generated and projective as an  $R$ -module, we define the *trace*  $\mathrm{tr}_{S/R}: S \rightarrow R$  to be the following composite

$$S \xrightarrow{\rho} \mathrm{End}_R(S) \xrightarrow{\mathrm{ev}} R.$$

**Proposition A.3.** In the setting of [Definition A.2](#), the following are equivalent:

- (1)  $f: R \rightarrow S$  is finite étale
- (2) The trace pairing  $(x, y) \mapsto \mathrm{tr}_{S/R}(x \cdot y)$  is non-degenerate
- (3)  $S/\mathfrak{m}$  is a finite separable field extension over  $R/\mathfrak{m}$  for every maximal ideal  $\mathfrak{m} \leq R$ .

If  $R$  is Noetherian, we furthermore have

- (4)  $S$  is projective as an  $S \otimes_R S$ -module.

If  $S$  is irreducible<sup>4</sup> and  $R = S^G$  for some finite subgroup  $G \leq \mathrm{Aut}_R(S)$ , then we equivalently have

- (5)  $R \rightarrow S$  is Galois with Galois group  $G = \mathrm{Aut}_R(S)$ .

*Proof.* The equivalence of [1](#), [2](#), and [3](#) is in [Knu91, I.7.3.3] and [Knu91, III.5.1.10], where these conditions are taken as a *definition* of finite and étale. We'd like to justify this agrees with the map of schemes being finite and étale. Since  $S$  is finitely generated and projective over  $R$ , it is flat, and the condition on residue fields provides that the map is unramified. Hence we see  $R \rightarrow S$  is finite, flat and unramified, i.e. finite étale.

If  $R$  is Noetherian then [AG60, 4.7] states that [4](#) and [3](#) are equivalent.

By [AG60, 1.3], separability is equivalent to the ring extension being Galois, provided all the elements of  $G = \mathrm{Aut}_R(S)$  are *strongly distinct* [AG60, 1.1]. In the case where  $S$  is irreducible, being strongly distinct and distinct as functions agree, which is clearly satisfied.  $\square$

## APPENDIX B. ON MINKOWSKI'S THEOREM

We saw in [Example 2.5](#) that there are no nontrivial étale ring extensions of  $\mathbb{Z}$ , and this reduced to proving that for any number field  $K$ , we have that  $\mathbb{Z} \rightarrow \mathcal{O}_K$  cannot be étale.

**Theorem B.1** ([Neu02, III.2.12]). A prime  $p$  ramifies in  $K/\mathbb{Q}$  if and only if  $p \mid \Delta_K$ .

See [this note of K. Conrad](#) for a proof.

<sup>4</sup>By irreducibility we mean  $\mathrm{Spec}(R)$  is irreducible, i.e. the only idempotents in  $R$  are 0 and 1.

The discriminant measures the size of a lattice attached to a number field – specifically, we look at all the real and complex embeddings, and we get a map

$$K \rightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

The image of  $\mathcal{O}_K$  is a lattice isomorphic to  $\mathbb{Z}^{r_1} \times \mathbb{Z}^{2r_2}$ . The volume of its fundamental domain in  $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$  is  $\sqrt{|\Delta_K|}$ .

So it suffices for us to prove that for any number field  $K$ , the discriminant  $\Delta_K$  has a prime divisor. A consequence of Minkowski’s theorem is a lower bound on  $\Delta_K$  for any number field  $\mathbb{Q} \subseteq K$  of rank  $n$ :

$$|\Delta_K| \geq \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}.$$

We check for  $n \geq 2$  that this lower bound is  $> 1$ .

## REFERENCES

- [AG60] Maurice Auslander and Oscar Goldman, *The Brauer group of a commutative ring*, Transactions of the American Mathematical Society **97** (1960), 367–409.
- [Ban17] Romie Banerjee, *Galois descent for real spectra*, Journal of Homotopy and Related Structures **12** (2017), no. 2, 273–297.
- [BD10] Mark Behrens and Daniel Davis, *The homotopy fixed point spectra of profinite Galois extensions*, Transactions of the American Mathematical Society **362** (2010), no. 9, 4983–5042.
- [CHR65] S. U. Chase, D.K. Harrison, and Alex Rosenberg, *Galois theory and cohomology of commutative rings*, Memoirs of the American Mathematical Society, no. 52, American Mathematical Society, Providence, R.I, 1965.
- [JT84] André Joyal and Myles Tierney, *An extension of the Galois theory of Grothendieck*, online-ausg ed., Memoirs of the American Mathematical Society, no. volume 309, American Mathematical Society, Providence, R.I, 1984.
- [Knu91] Max-Albert Knus, *Quadratic and Hermitian forms over rings*, Grundlehren Der Mathematischen Wissenschaften, vol. 294, Springer-Verlag, 1991.
- [Mat16] Akhil Mathew, *The Galois group of a stable homotopy theory*, Advances in Mathematics **291** (2016), 403–541.
- [Mei12] Lennart Meier, *United Elliptic Homology*, Ph.D. thesis, Rheinischen Friedrich-Wilhelms-Universität Bonn, 2012.
- [Neu02] Jürgen Neukirch, *Algebraische Zahlentheorie*, 1. nachdr. ed., Springer, Berlin Heidelberg, 2002.
- [RG71] Michel Raynaud and Laurent Gruson, *Critères de platitude et de projectivité*, Inventiones mathematicae **13** (1971), no. 1, 1–89.
- [Rog08a] John Rognes, *A Galois extension that is not faithful*.
- [Rog08b] ———, *Galois extensions of structured ring spectra. Stably dualizable groups*, Memoirs of the American Mathematical Society **192** (2008), no. 898, 0–0.