GALOIS NOTES

NILES JOHNSON

Abstract. This is a collection of notes from our reading project on Galois theory for rings and ring spectra. An attempt is made to outline main ideas and give references, but only a minimal effort has been put into checking details.
Many thanks are due to the various people who participated; without their interest, we certainly wouldn't have made it even this far.

1. Review for rings

1.1. **Revisionist Galois theory for fields.** Let L/K be an extension of fields, and G a finite group. Then L/K is G-Galois if $G = \mathrm{Aut}(L/K)$ and $K = L^G$. In this situation there is a bijection between subgroups $H \leq G$ and intermediate fields $L/F/K$.

Here are two results from Galois theory for fields which find generalizations in the theory for rings:

- Hilbert's theorem 90: $H^1(G, U(L)) = 0$, where $U(L) = L^\times$ denotes the group of units in L.
- $Br(K) = H^2(K^{sep}/K, U(K^{sep}))$.

To prepare for the generalization to rings, we make a couple of definitions and reformulate the Galois condition.

Definition 1.2 (Twisted Group Ring)**.** As an L-vector space, $L\langle G\rangle$ is $L \times G$. The multiplication is twisted by the action of G:

$$(x, g) \cdot (y, h) = (xg(y), gh).$$

Note that there is a natural map

$$j : L\langle G\rangle \to \mathrm{Hom}_K(L, L)$$

given by

$$(x, g) \mapsto (t \mapsto x \cdot g(t)).$$

This is adjoint to the action of L on $L\langle G\rangle$:

$$L \otimes L\langle G\rangle \to L.$$

Proposition 1.3. *The map j is a K-algebra homomorphism and is bijective if and only if L/K is G-Galois.*

Idea of proof. Dedekind's lemma says that

$$\mathrm{Alg}_K(A, L) \subset \mathrm{Hom}_K(A, L)$$

is a linearly independent subset, so j is injective. When L/K is Galois, j is surjective by a dimension count. For details see [Dre95]. ... □

Notation 1.4. Let $L^{\times G}$ denote $\prod_G L$, set maps from G to L.

Date: September 2010.

There is a natural map

$$h : L \otimes_K L \to L^{\times G}$$

given by

$$(x \otimes y) \mapsto (x \cdot g(y))_{g \in G}.$$

Proposition 1.5. *The map h is an L-algebra homomorphism, and is bijective if and only if L/K is G-Galois.*

Idea of proof. The map h is the L-module dual of j:

$$\mathrm{Hom}_L(L \otimes_K L, L) \cong \mathrm{Hom}_K(L, L)$$

and

$$\mathrm{Hom}_L(L^{\times G}, L) \cong L\langle G \rangle.$$

$\ldots \square$

1.6. **Basic definitions and theorems for rings.** Most of this subsection is based on Chapter 0 of Greither [Gre92].

The following theorem generalizes the previous results for fields; part *ii* is taken as the definition of G-Galois.

Theorem 1.7. *For a map (inclusion) of commutative rings $R \to T$, and a finite group $G \leq \mathrm{Aut}_{R\text{-}alg}(T)$, suppose $R \cong T^G$. Then the following are equivalent:*

i. T is finitely-generated and projective over R and
$j : T\langle G \rangle \to Hom_R(T, T)$ is an isomorphism (of R-algebras).
ii. $h : T \otimes_R T \to T^{\times G}$ is an isomorphism (of T-algebras).
(This implies that T is finitely-generated and projective over R.)

Remark 1.8. Note that the Galois correspondence (Theorems 1.19 and 1.20) implies that in this case $G = \mathrm{Aut}_{R\text{-alg}}(T)$.

The following property is essential in many of the applications of Galois extensions:

Lemma 1.9. *If T/R is G-Galois, then T is faithfully flat over R ($T \otimes_R -$ preserves and detects exact sequences).*

Idea of proof. Use Nakayama's lemma: $T/\mathfrak{m}T \neq 0$ because $T_{\mathfrak{m}} \neq 0$ ($R_{\mathfrak{m}} \subset T_{\mathfrak{m}}$). $\ldots \square$

The following results illustrate some of the benefits of faithful-flatness. Note however that this situation does not generalize to topological Galois extensions. Check the counterexamples of Wieland or Baker-Richter: Section 4.1, [BR10].

Proposition 1.10. *Let L be faithfully flat over R, and suppose that G is a group acting on T/R. If $L \otimes_R T/L$ is G-Galois, then T/R is G-Galois.*

Note. It is important here that the G-action is induced by that on T/R; $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has a trivial $\mathbb{Z}/3$ action, and hence extending scalars will always result in a trivial $\mathbb{Z}/3$ action.

Lemma 1.11. *The trace map $tr : T \to R$ splits R as a summand of T*

Note. The previous result does not generalize to the topological setting.

Lemma 1.12. *Let T/R and T'/R be G-Galois extensions. Then every map of G-Galois extensions $\varphi : T \to T'$ is an isomorphism.*

Idea of proof. Flat base change to the case of a trivial extension (which can always be done), and without loss of generality take R to be local. In that case, one can construct an orthogonal basis and check directly that φ is an isomorphism. ...□

Lemma 1.13. *Let T/R be G-Galois. Then T is a finitely-generated projective R-module of rank 1 (an invertible module) over the group ring $R[G]$.*

Idea of proof.

$$T[G] \otimes_{R[G]} T \cong T \otimes_R T \cong T^{\times G}$$

Now $T^{\times G}$ is invertible over $T[G]$, and hence we are done by faithfully flat descent. ...□

1.14. **Galois correspondence.** The Galois correspondence for rings requires a couple of additional definitions; this could probably be explained more clearly using the language of Galois connections.

Definition 1.15. An R-algebra A is called *separable* over R if A is projective over $A^e := A \otimes_R A^{op}$.

Definition 1.16. Suppose G acts on T/R. Two elements $\sigma, \tau \in G$ are called *strongly distinct* if for every non-zero idempotent $e \in T$ there is some $x \in T$ such that $e \cdot \sigma(x) \neq e \cdot \tau(x)$. Note that if T has no non-trivial idempotents then strongly distinct is the same as distinct.

Definition 1.17. T is called *connected* if it has no non-trivial idempotents

Definition 1.18. Suppose T/R is G-Galois and let U be an intermediate ring. We say that U is G-strong if the restrictions to U of any two elements of G are either strongly distinct or equal.

The following theorems come from the first chapter of [CHR65]. As done there, we put in brackets those statements which are vacuous in the case that T is connected.

Theorem 1.19. *For T/R G-Galois and $H \leq G$, let $U = T^H$. Then*

i. U is separable over R [and G-strong].
ii. T/U is H-Galois.
iii. $H = \mathrm{Aut}(T/U)$.
iv. if $H \triangleleft G$ then U/R is G/H-Galois.

Idea of proof. Let $\delta\colon T \to T^{\times G}$ be the T-module map induced by sending the unit of T to $(\delta_{e\sigma})_{\sigma \in G}$, the element which has a 1 in the e-coordinate and 0's elsewhere. The isomorphism $h_{T/R}$ gives a lift in the diagram below.

$$\begin{array}{ccc} & & T \\ & \swarrow & \downarrow{\scriptstyle \delta} \\ T \otimes_R T & \xrightarrow[\cong]{h_{T/R}} & T^{\times G} \\ \downarrow & & \downarrow \\ T \otimes_U T & \xrightarrow{h_{T/U}} & T^{\times H} \end{array}$$

Now the lift imples that $h_{T/U}$ is surjective, which imples that $j_{T/U}$ is an isomorphism and hence T/U is H-Galois. To see that U/R is separable, we have the following: T/U Galois implies that T is finitely-generated and projective over $U \otimes_R U$, which implies that $T \otimes_R T$ is also finitely-generated and projective over $U \otimes_R U$. T/R Galois implies that T/R is separable, which is to say that T is finitely-generated and projective over $T \otimes_R T$. Now since T/U is Galois, U is a T-module summand of T and thus a $U \otimes_R U$-module summand of T. This implies that U is projective (and of course finitely-generated) over $U \otimes_R U$.

Let $H' = Aut(T/U)$. Then $H \leq H'$ and $T^H = U = T^{H'}$ so T/U is Galois for both H and H'. But the orders of H and H' give the rank of $T \otimes_U T$, and therefore $H = H'$.

If $H \triangleleft G$, in the case that $T = R^{\times G}$, one can see directly that $T^H \cong T^{\times G/H}$. By faithfully flat descent, this suffices. $\ldots \square$

Theorem 1.20. *Let T/R be G-Galois and U an intermediate ring which is separable over R [and G-strong]. Then there exists an $H \leq G$ such that $U = T^H$.*

Example 1.21. For L/K a G-Galois extension of number fields, $\mathscr{O}_L/\mathscr{O}_K$ is a G-Galois extension of rings if and only if L/K is unramified. For a maximal ideal $\mathfrak{p}$, one has a G-Galois extension $(\mathscr{O}_L)_\mathfrak{p}/(\mathscr{O}_K)_\mathfrak{p}$ if and only if L/K does not ramify at $\mathfrak{p}$.

Example 1.22. To see that the G-strong condition is necessary, consider the following: Let $T = \bigoplus_{i=1}^4 Re_i$ be a $\mathbb{Z}/4$-extension where the e_i are pairwise orthogonal idempotents with $\Sigma e_i = 1$ and with the generator σ cyclicly permuting the e_i. Now let $U = R(e_1 + e_2) \oplus R(e_3 + e_4)$. Then $\mathrm{Aut}(T/U)$ is trivial, but the intermediate ring fixed by the trivial group is T, not U.

2. Units-Picard-Brauer for rings

The results of this section are contained in the AMS memoir of Chase–Harrison–Rosenberg [CHR65], mostly in the second chapter.

Note. Throughout this section, R will be a fixed commutative ring and $\otimes$ will denote $\otimes_R$.

2.1. The Brauer group.

Throughout this subsection, we consider a (noncommutative) R-algebra A. We begin with some definitions and a lemma:

Definitions 2.2.

- A is called *separable* over R if A is projective as a module over A^e. Since A is always finitely generated over A^e, this is equivalent to the condition that A be a dualizable module over A^e. By the dual basis lemma, this is equivalent to the condition that the coevaluation
$$A \otimes_{A^e} \mathrm{Hom}_{A^e}(A, A^e) \to \mathrm{Hom}_{A^e}(A, A)$$
be an isomorphism. To motivate this term, it should be noted that when R is a field, A being separable over R implies that A is semi-simple over R and remains semi-simple upon extension of scalars over any field extension of R. When A is also a field, this implies that A is a separable extension of R in the usual sense for fields [Coh03].
- A is called *central* over R if the center of A is precisely R; this occurs if and only if the unit
$$R \to \mathrm{Hom}_{A^e}(A, A)$$
is an isomorphism.
- A is called *faithfully projective* over R if both the coevaluation
$$\mathrm{Hom}_R(A, R) \otimes A \to \mathrm{Hom}_R(A, A)$$
and the evaluation
$$A \otimes_{A^e} \mathrm{Hom}_R(A, R) \to R$$
are isomorphisms. Note, again by the dual basis lemma, that the coevaluation being an isomorphism is equivalent to A being finitely-generated and projective as an R-module. The evaluation map being an isomorphism implies that $- \otimes_R A$ is faithful in the sense that $M \otimes_R A = 0$ implies $M = 0$.

Lemma 2.3 (See e.g. [KO74] or [DI71])**.** *If A is central and separable over R, then the evaluation*
$$\mathrm{Hom}_{A^e}(A, A^e) \otimes_R A \to A^e$$
is an isomorphism.

An R-algebra A satisfying any (and therefore all) of the following conditions is called Azumaya over R. The Brauer group of R, $Br(R)$, is the group of Morita equivalence classes of Azumaya R-algebras. The fact that this is a group follows from the definition of Azumaya.

Theorem 2.4. *The following are equivalent:*

i. A is an invertible (R, A^e)-bimodule and thus A^e is Morita equivalent to R.
ii. A is central and separable over R.
iii. A is faithfully projective over R and the "sandwich map" (unit)

$$A^e \to \mathrm{Hom}_R(A, A)$$

is an isomorphism.
iv. There is an R-algebra B such that $A \otimes_R B$ is Morita equivalent to R.

For an extension of commutative rings S/R, the relative Brauer group is the group of Azumaya R-algebras (up to Morita equivalence) which split upon extension to S:

$$Br(R, S) = Br(S/R) := ker(Br(R) \xrightarrow{S\otimes_R -} Br(S)).$$

2.5. **Rigifying the Brauer group.** In this subsection we identify some particular Abelian groups covering $Br(R, S)$. This is motivated by the following:

Lemma 2.6 (Splitting Lemma)**.** *If A/R is Azumaya and S is the maximal commutative sub-R-algebra of A, then $S \otimes A^{op} \cong \mathrm{End}_S(A)$ and hence $A \in Br(R, S)$.*

Idea of proof. First show that if $h : B \to B'$ is a map of Azumaya R-algebras and $im(h)$ contains its centralizer in B, then h is an isomorphism. Now $S \otimes A^{op}$ is Azumaya over S, as is $\mathrm{End}_S(A)$, and there is an obvious map $S \otimes A^{op} \to \mathrm{End}_S(A)$. The centralizer of the image is the collection of endomorphisms given as left-multiplication by an element of S, and thus this map is an isomorphism. $\ldots \square$

Now we describe a collection of Azumaya algebras which are split in a specific way. Let $\mathcal{CAlg}_R$ denote the category of commutative R-algebras, and $\mathcal{CAlg}_R^{f.p.}$ the full subcategory of commutative R-algebras which are faithfully projective as R-modules. Later, we will also make reference to the full subcategory of faithfully flat commutative R-algebras, $\mathcal{CAlg}_R^{f.f.}$. Let $A(S, T)$ denote the following set:

$$A(S,T) := \{A \text{ Azumaya over } T \text{ with } i_A : S \otimes T \hookrightarrow A \text{ maximal commutative}\}/(\cong \text{ under } S \otimes T)$$

So A and B are equivalent in $A(S, T)$ if there is an isomorphism of algebras commuting with the given inclusions of $S \otimes T$:

$$\begin{array}{ccc} & S \otimes T & \\ \swarrow & & \searrow \\ A & \xrightarrow{\cong} & B \end{array}$$

The sets $A(S, T)$ can be made functorial: for a map $(S, T) \to (S', T')$ in $\mathcal{CAlg}_R^{f.p.} \times \mathcal{CAlg}_R$, we define a map

$$\begin{aligned} A(S,T) &\to A(S,T) \text{ by} \\ A &\mapsto A' = \mathrm{End}_A(S' \otimes_S A) \otimes_T T' \\ &\cong \mathrm{End}_{A\otimes_T T'}(S' \otimes_S A \otimes_T T') \end{aligned}$$

where $S' \otimes T' \to A'$ is defined by (left-mult. $\otimes$ 1). Note that A' and $A \otimes_T T'$ represent the same class in $Br(T')$ [CHR65, II.2.7].

Furthermore, $A(S, T)$ has a naturally defined product: for $A, B \in A(S, T)$, $A \otimes_T B$ is an element of $A(S \otimes S, T)$, and the algebra structure of S induces a map $A(S \otimes S, T) \to A(S, T)$.

Example 2.7. Let J be an invertible module over $S \otimes T$ (finitely-generated projective of rank 1). Then $\mathrm{End}_T(J)$ is an element of $A(S,T)$. In particular, let $D = \mathrm{End}_T(S \otimes T)$.

Proposition 2.8. *Each $A(S,T)$ is a commutative monoid with unit $D = \mathrm{End}_T(S \otimes T)$ and there is an exact sequence of commutative monoids*

$$Pic(R) \to Pic(S) \to A(S,R) \to Br(R,S) \to 0$$

Idea of proof. $A(S,R)$ maps to $Br(R,S)$ by the splitting lemma (2.6). ...□

Corollary 2.9. *By a diagram chase, $A(S,R)$ is an abelian group.*

Now to close this subsection, we have something like a filtration for $A(S,R)$ and $Pic(S)$:

Definition 2.10.

$$KA(S,T) := ker(A(S,R) \to A(S,T))$$
$$KPic(S,T) := ker(Pic(S) \to Pic(S \otimes T))$$

Proposition 2.11. *For $S \in \mathcal{CAlg}_R^{f.p.}$ we take colimits over $T \in \mathcal{CAlg}_R$: everything splits eventually.*

i. $Pic(S) = \operatorname{colim}_T KPic(S,T)$

ii. $A(S,R) = \operatorname{colim}_T KA(S,T)$

2.12. **Functors to $\mathcal{Ab}$.** The following functors to the category of abelian groups are of interest.

- The units functor $U : \mathrm{Alg}_R \to \mathcal{Ab}$
- The Picard functor $Pic : \mathcal{CAlg}_R \to \mathcal{Ab}$
- The Brauer functor $Br(R,-) : \mathcal{CAlg}_R \to \mathcal{Ab}$
- $A(-,-) : \mathcal{CAlg}_R^{f.p.} \times \mathcal{CAlg}_R \to \mathcal{Ab}$

In the previous subsection, we also saw $KPic$ and KA. In this subsection we describe some general constructions for functors

$$F : \mathcal{CAlg}_R \to \mathcal{Ab}.$$

First, regard F as a functor of two variables by

$$F(S,T) = F(S \otimes T).$$

Now we make the following definitions:

$$\begin{aligned} QF(S,T) &= coker(F(T) \to F(S \otimes T)) \\ Q^nF(S,T) &= QF(S^{\otimes n-1}, T) \\ &= coker(F(S^{\otimes n-1} \otimes T) \to F(S^{\otimes n} \otimes T)) \end{aligned} \tag{2.13}$$

Thus we have the following commutative diagram with exact rows:

$$\begin{array}{ccccc} F(T) & \longrightarrow & F(S \otimes T) & \longrightarrow & QF(S,T) \\ \downarrow & & \downarrow{\scriptstyle \varepsilon_1} & & \downarrow{\scriptstyle \Delta_1} \\ F(S \otimes T) & \xrightarrow{\varepsilon_0} & F(S^{\otimes 2} \otimes T) & \longrightarrow & Q^2F(S,T) \\ \downarrow{\scriptstyle \varepsilon_0 - \varepsilon_1} & & \downarrow{\scriptstyle \varepsilon_1 - \varepsilon_2} & & \downarrow{\scriptstyle \Delta_2} \\ F(S^{\otimes 2} \otimes T) & \xrightarrow{\varepsilon_0} & F(S^{\otimes 3} \otimes T) & \longrightarrow & Q^3F(S,T) \end{array}$$

The maps ε_i are induced by using the unit map $R \to S$ in the i^{th} factor of $S^{\otimes k} \to S^{\otimes k+1}$. Note that the difference of the vertical and horizontal maps to $F(S^{\otimes 3} \otimes T)$ is the differential in the Amitsur complex (defined below).

We end this subsection with one more definition:

$$KF(S,T) = ker(\Delta_2). \tag{2.14}$$

Note that $\Delta_2\Delta_1 = 0$, so there is an induced natural transformation $\Delta\colon QF \to KF$.

Remark 2.15 (Warning). Although the notation is similar to that for $KPic$ and KA, these are defined in the previous subsection. These are the original notations in [CHR65], and we do not know if the similarity is meaningful.

Recall that $D = \mathrm{End}_R(S)$ is the unit of $A(S,R)$; $D \otimes T \cong \mathrm{End}_T(S \otimes T)$ is the unit of $A(S,T)$.

Lemma 2.16. $KU(S,T) \cong \mathrm{Aut}_{A(S,T)}(D \otimes T)$.

Idea of proof. For $u \in U(S^{\otimes 2} \otimes T)$ representing a class in $KU(S,T)$, we have u acting on $D \otimes T$ by conjugation. This correspondence gives the isomorphism. ...□

Lemma 2.17. *For $S \in \mathcal{CAlg}_R^{f.p.}$ and $T \in \mathcal{CAlg}_S$, the induced map*

$$\Delta\colon QU(S,T) \to KU(S,T)$$

is an isomorphism.

Idea of proof. Use the multiplication $S^{\otimes 3} \otimes T \xrightarrow{1\otimes 1\otimes \mathrm{mult}} S^{\otimes 2} \otimes T$ to show that Δ is surjective. ...□

3. The Amitsur complex for rings

Note. The content of this section comes from Chapter II of [CHR65], written by Chase and Rosenberg.

The Amitsur complex is a cosimplicial complex defined by

$$AC^\bullet(S/R) : [q] \mapsto S^{\otimes q+1}$$

with the usual cofaces and codegenericies given by unit maps and multiplications. A cochain complex is constructed from this data by taking alternating sums of the coface maps.

If F is a functor to $\mathcal{Ab}$, we define $AC^\bullet(S/R;F)$ by applying F termwise. The cohomology of the resulting complex is the Amitsur cohomology $AH^*(S/R;F)$.

Lemma 3.1. *If $f, f'\colon T \to T'$ are commutative R-algebra maps, then f and f' induce chain homotopic maps on $AC^\bullet(T/R;F)$. Thus if T' is a commutative R-algebra retract of T, then $AH^*(T'/R;F)$ is a retract of $AH^*(T/R;F)$.*

Remark 3.2. The definition of the Amitsur complex makes sense for spectra and is discussed in [Rog08, §8.2]. For $A \to B$ an extension of S-algebras (S the sphere spectrum here), $A^\wedge_B := Tot(AC^\bullet(B/A))$ is a completion of A along the map to B, and this completion agrees with Bousfield B-nilpotent completion.

Moreover, for G acting on B/A we have $h^\bullet : AC^\bullet(B/A) \to C^\bullet(G;B)$ induced by

$$h : B \wedge_A B \to F(G_+, B)$$

(F the function spectrum here). If h is a weak equivalence, then $h^\bullet$ is codegreewise a weak equivalence and induces a weak equivalence on Tot. We have $Tot(C^\bullet(G;B)) = B^{hG}$ and thus the Galois question can be analyzed by considering the following:

$$\begin{array}{ccc} & & A^\wedge_B \\ & \nearrow & \downarrow Tot(h^\bullet) \\ A & \xrightarrow{i} & \\ & \searrow & B^{hG} \end{array}$$

Now we return to the case of commutative rings.

3.3. **Identifying terms.** In this subsection, we consider $AH^n(T/R; G_S)$ for functors G_S such as

- $F_S = F(S \otimes -)$.
- $QF_S = QF(S, -)$.
- $KF_S = KF(S, -)$.

In our applications we will take $F = U$ or $F = Pic$.

Definition 3.4. For a functor F to $\mathcal{Ab}$, we define

$$AH^n(R; F) = \operatorname*{colim}_T AH^n(T/R; F)$$

and

$$AHF^*(S) = \operatorname*{colim}_T AH^*(T/R, F_S).$$

Theorem 3.5. *There is a natural transformation $\psi : KA(S,T) \to AH^1(T/R; KU_S)$ which is an equivalence on $\mathcal{CAlg}_R^{f.p.} \times \mathcal{CAlg}_R^{f.f.}$.*

Idea of proof. Let $A \in KA(S,T)$, so $S \otimes R \to A$ maximal commutative and we have

$$\begin{array}{ccc} & S \otimes T & \\ \swarrow & & \searrow \\ D \otimes T & \xrightarrow[\cong]{g} & A \otimes T \end{array}$$

(recall that D is the unit in $A(S,R)$). We define $\psi(A) = \bar{u} \in AC^1(T/R; KU_S)$ as follows: Let j be the composite

$$j : D \otimes T^{\otimes 2} \xrightarrow[\cong]{g} A \otimes T^{\otimes 2} \xrightarrow{1 \otimes \tau} A \otimes T^{\otimes 2} \xrightarrow[\cong]{g^{-1}} D \otimes T^{\otimes 2} \xrightarrow{1 \otimes \tau} D \otimes T^{\otimes 2}.$$

Then there is some $u \in U(S^{\otimes 2} \otimes T^{\otimes 2})$ whose image $\bar{u}$ in $KU(S, T^{\otimes 2}) \subset Q^2U(S \otimes T^{\otimes 2})$ has the property that

$$j(x) = \bar{u}\, x\, \bar{u}^{-1}$$

(recall Lemma 2.16: automorphisms in $A(S, T^{\otimes 2})$ are inner, by elements of $KU(S, T^{\otimes 2})$). Check that $\bar{u}$ is a cocycle. ...□

Corollary 3.6. *For each $S \in \mathcal{CAlg}_R^{f.p.}$, and each $T \in \mathcal{CAlg}_S^{f.f.}$, the transformation ψ above induces a natural isomorphism $\psi : KA(S,T) \to AH^1(T/R; QU_S)$.*

Idea of proof. Use the isomorphism of Lemma 2.17. ...□

Theorem 3.7. *There is a natural transformation $\varphi : KPic(S,T) \to AH^1(T/R; U_S)$ which is an equivalence on $\mathcal{CAlg}_R^{f.p.} \times \mathcal{CAlg}_R^{f.f.}$.*

Idea of proof. Let $J \in KPic(S,T)$, so $J \in Pic(S)$ and we have

$$S \otimes T \xrightarrow[\cong]{g} J \otimes T.$$

We define $\varphi(J) = u \in U(S \otimes T^{\otimes 2}) = AC^1(T/R; U_S)$ as follows: Let j be the composite

$$j : S \otimes T^{\otimes 2} \xrightarrow[\cong]{g} J \otimes T^{\otimes 2} \xrightarrow{1 \otimes \tau} J \otimes T^{\otimes 2} \xrightarrow[\cong]{g^{-1}} S \otimes T^{\otimes 2} \xrightarrow{1 \otimes \tau} S \otimes T^{\otimes 2}.$$

Then there is some $u \in U(S \otimes T^{\otimes 2})$ such that

$$j(x) = u\, x.$$

Check that u is a cocycle. ...□

Lemma 3.8. *The following comparison diagram commutes for $S \in \mathcal{CAlg}_R^{f.p.}$ and $T \in \mathcal{CAlg}_S^{f.f.}$.*

$$\begin{array}{ccc} KPic(S,T) & \longrightarrow & KA(S,T) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} \\ AH^1(T/R;U_S) & \xrightarrow{AH^1(proj.)} & AH^1(T/R;QU_S) \end{array}$$

Remark 3.9. [CHR65] Makes reference to an alternative technique for a unified proof of the previous two theorems, using various fibered categories over $\mathcal{CAlg}_R^{f.p.} \times \mathcal{CAlg}_R$ and analyzing the distinguished object X_0 of each. In each case one has

$$Aut(X_0)(T) \cong Aut(X_0 \otimes T)$$

and a comparison with $H^n(T/R, Aut(X_0))$.

Theorem 3.10.

i. The following sequence is exact.

$$\begin{array}{ccccccccc} Pic(R) & \longrightarrow & Pic(S) & \longrightarrow & A(S,R) & \longrightarrow & Br(R,S) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ AHU^1(R) & \longrightarrow & AHU^1(S) & \longrightarrow & AHQU^1(S) & \longrightarrow & AHU^2(R) & \longrightarrow & AHU^2(S) \end{array}$$

ii. As functors of $S \in \mathcal{CAlg}_R^{f.p.}$, we have natural transformations

$$\begin{array}{cccccccc} U(S) & & KPic(S,T) & \longrightarrow & Pic(S) & KA(S,T) & \longrightarrow & A(S,R) \\ \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \varphi_T} & & \downarrow{\scriptstyle \operatorname{colim}\varphi_T} & \downarrow{\scriptstyle \psi_T} & & \downarrow{\scriptstyle \operatorname{colim}\psi_T} \\ AHU^0(S) & & AH^1(T/R;U_S) & \longrightarrow & AHU^1(S) & AH^1(T/R;QU_s) & \longrightarrow & AHQU^1(S) \end{array} \qquad \begin{array}{c} Br(R,S) \\ \vdots \\ \downarrow \\ AHU^2(R) \end{array}$$

iii. The following sequence is exact.

$$0 \to Br(R,S) \to AHU^2(R) \to AHU^2(S)$$

Idea of proof.

i. Exactness of the top row follows from the definition of $A(S,T)$. Exactness of the bottom row follows from the long exact sequence in homology induced by the short exact sequence

$$0 \to U \to U_S \to QU(S,-) \to 0$$

for $S \in \mathcal{CAlg}_R^{f.p.}$.

ii. $AHU^2(R)$ is a constant functor of S, and the dashed map follows from existence of the others by exactness of part (i).

$\ldots \square$

3.11. **Spectral sequence.** First we introduce the bigraded Amitsur complex:

$$C^{p,q}(S,T/R;F) = F(S^{\otimes p+1} \otimes T^{\otimes q+1}).$$

Then we have a spectral sequence

$$AH^p(S/R;AH_TF^q) \Rightarrow H^{p+q}C^\bullet(S,T/R,F)$$

where $AH_TF^q(S) = AH^q(T/R;F_S)$.

Lemma 3.12. *If T is an S-algebra, then*

$$H^{p+q}C^\bullet(S,T/R,F) \cong AH^{p+q}(T/R;F).$$

Idea of proof. This follows from Lemma 3.1. $\ldots \square$

Taking the colimit defining $AH^*(R;F)$ over S-algebras T, we have

$$AH^p(S/R; AHF^q) \Rightarrow AH^{p+q}(R;F). \tag{3.13}$$

Lemma 3.14. *Let $E_r^{p,q} \Rightarrow H^{p+q}$ be a first-quadrant spectral sequence. Then there is a 7-term exact sequence*

$$0 \longrightarrow E_2^{1,0} \longrightarrow H^1 \longrightarrow E_2^{0,1} \longrightarrow E_2^{2,0} \longrightarrow \mathrm{F}^1H^2 \longrightarrow E_2^{1,1} \longrightarrow E_2^{3,0}$$

where F^1H^2 is the first filtration group.

Corollary 3.15. *Taking $F = U$ in the spectral sequences above, we have*

$$0 \longrightarrow AH^1(S/R;U) \longrightarrow Pic(R) \longrightarrow AH^0(S/R;Pic) \longrightarrow AH^2(S/R;U) \longrightarrow$$

$$\longrightarrow Br(R,S) \longrightarrow AH^1(S/R;Pic) \longrightarrow AH^3(S/R;U).$$

Idea of proof. To identify the first filtration group as $Br(R,S)$, note that the inclusion $r\colon T \to S\otimes T$ induces a commuting map

$$\begin{array}{ccc} AH^*(T/R;F) & & \\ \downarrow{\scriptstyle \eta} & \searrow^{r} & \\ H^*C^\bullet(S,T/R,F) & \longrightarrow & AH^*(T/R;F_S). \end{array}$$

If T is an S-algebra, then η is an isomorphism and hence $ker(r) \cong \mathrm{F}^1AH^*(T/R;F_S)$. Passing to colimits over S-algebras T gives $\mathrm{F}^1AH^n(R;F) = ker(AH^n(R;F) \to AH^n(R;F_S))$. By Theorem 3.10 (*iii*), this kernel is $Br(R,S)$. ...□

3.16. **Galois extensions.**

Theorem 3.17 ([CHR65, Theorem I.5.4])**.** *For S/R G-Galois, we have*

$$H^*(S/R;U) \cong H^*(G;U(S))$$
$$H^*(S/R;Pic) \cong H^*(G;Pic(S)).$$

4. Highly structured ring spectra

Spectra are representing objects for generalized cohomology theories on based spaces. Naturally isomorphic cohomology theories correspond to homotopy equivalent spectra, and cohomology theories with product structures correspond to ring spectra. To develop the Galois theory of ring spectra, it is necessary to work in a category of highly-structured spectra: a closed monoidal category with a notion of homotopy such that its homotopy category is equivalent to the category of spectra (cohomology theories). Monoid objects in such a category are highly-structured ring spectra, and there is a natural theory of module spectra over these ring spectra, etc. There are a number of different constructions which give categories of highly-structured spectra, but we will not say more about that here.

4.1. **Non-Faithfulness of Galois Extensions.**

Definition 4.2. An extension of rings $A \to B$ is faithful if, for any A-module M,

$$M \wedge_A B \simeq * \quad \Rightarrow \quad M \simeq *$$

The following example is due to Ben Wieland, although the fact that this is a Galois extension, and the proposition with which to prove it is non-faithful, are both contained in [Rog08].