Algebraic Preliminaries
Reductive Algebraic Groups - II

Anupam Singh

Contents

1. Introduction

These notes are based one Chapter 11 of the Springer's [Sp] book and are meant to be background material needed for the theory of algebraic groups over base field.

In this note we denote k a field and F a subfield of it. Mostly k denotes an algebraically closed field. To be consistent with the notation from theory of algebraic groups over algebraically closed field k we will mean X to be a variety over k though strictly speaking it should be $X(k)$ and similarly a vector space V will mean a k-vector space but a vector space W over F will be called an F-vector space W or W a F-space.

1.1. F-Functors and Affine Schemes.

An F-functor is a functor from category of F-algebras to the category of sets. For any F-algebra R, we can define an F-functor Sp_FR through $(Sp_FR)(A) = \mathrm{Hom}_{F-alg}(R, A)$. We call Sp_FR the spectrum of R. Any F-functor isomorphic to some Sp_FR is called an **affine scheme over** F. Or equivalently a functor X is called **representable** or represented by R if it is an affine scheme, i.e., $X(A) = \mathrm{Hom}_{F-alg}(R, A)$. We also have Yonenda's Lemma: For any F-algebra R and any F-functor X, there is a bijection

$$Mor(Sp_F R, X) \cong X(R).$$

We define $F[X] := Mor(X, \mathbb{A}^1)$ which is the corresponding affine algebra in case X is an affine scheme. For two F-schemes X and X' we have $Mor(X, X') \cong \mathrm{Hom}_{F-alg}(F[X], F[X'])$.

This way we think of any affine algebraic variety X defined over F as an affine scheme $Sp_F F[X]$. For an F-algebra E we have base-change from F to E for a scheme X which is denoted as X_E given by $X_E(A) = X(A)$.

2. F-structures

In this section we define F-structures on algebraic objects. The philosophy is as follows: to study algebraic objects over algebraically closed fields (k) are simpler and hence to study the same property/question over arbitrary fields (F) we try to push down the property/question from k to F.

2.1. **F-structures on Vector Spaces.**

Let k be a field (not necessarily algebraically closed). Let V be a (k-space) vector space.

Definition 2.1.1. *An F-**structure** on V is a subspace V_0 of F-vector space V such that the canonical homomorphism $k \otimes_F V_0 \to V$ is a k-isomorphism.*

We shall denote $V(F) := V_0$. A vector space with F-structure will be called an F**-vector space**. A liner map $f \colon V \to W$ of F-vector spaces is defined over F if f maps $V(F)$ to $W(F)$. A subspace W of V is an F-subspace if it has a basis whose elements lie in $V(F)$.

Example 2.1.2. $M_2(\mathbb{C})$ is a 4-dimensional vector space over $\mathbb{C}$. $M_2(\mathbb{R})$ and

$$\mathbb{H} = \left\{ \begin{pmatrix} z & -w \\ \bar{w} & \bar{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\}$$

are $\mathbb{R}$ structures on $M_2(\mathbb{C})$. As a vector spaces they are isomorphic but not as an algebra.

Exercise 2.1.3. Let V has an F-structure V_0. Prove that V has a basis consisting of elements of V_0. Moreover show that with this appropriate basis the k-linear maps correspond to matrices over k and F-maps correspond to the matrices over F.

Exercise 2.1.4. Prove following:

(1) Let W be an F-subspace of V. Then V/W is an F-space.
(2) Show also that direct sum and tensors of F-spaces are F-space again.
(3) Let $V(F)$ be an F-structure on V. Suppose $E \subset k$ is a field extension of F. Then $V(E) := E \otimes_F V(F)$ is an E-structure.

Exercise 2.1.5 (11.1.2 Springer)**.** V and W are F-vector spaces and $f \colon V \to W$ is a k-linear map.

(1) If f is defined over F then $ker(f)$ and $Im(f)$ are defined over F as well.
(2) The converse is false.
(3) f is defined over F if and only if its graph is an F-subspace of $V \oplus W$.

2.2. **F-structures on Varieties.** Let $X \subset k^n$ be a variety (closed set) with ideal $I(X)$. We say that F **is a field of definition** of X if $I(X)$ is generated by polynomials over F. However this is not an intrinsic definition. Let $A = k[X]$ be an affine algebra. An F**-structure** on X is an F-subalgebra A_0 of A which is of finite type over F and which is such that the homomorphism induced by multiplication $k \otimes_F A_0 \to k[X]$ is an isomorphism. We then denote $A_0 = F[X]$. For the given F-structure on X the set of F**-rational points** $X(F)$ is given by $X(F) = \mathrm{Hom}_{F-alg}(F[X], F)$. Obviously $X(k) = X$.

Example 2.2.1. Let $k = \mathbb{C}$ and $F = \mathbb{R}$. Let $k[X] = \frac{\mathbb{C}[T_1,T_2]}{<T_1^2+T_2^2-1>}$ and let a, b be the image of T_1 and T_2 in $k[X]$. Then $\mathbb{R}[a, b]$ and $\mathbb{R}[ia, ib]$ defines two different $\mathbb{R}$-structures on X. Notice that the first one correspond to the equation $T_1^2 + T_2^2 = 1$ and the second one to $T_1^2 + T_2^2 = -1$.

Example 2.2.2. Let $k = \mathbb{C}$ and $F = \mathbb{R}$. Let $k[X] = \frac{\mathbb{C}[T_{11},T_{12},T_{22},T_{21}]}{<T_{11}T_{22}-T_{12}T_{21}-1>}$ and let $a_{11}, a_{12}, a_{21}, a_{22}$ be the image of the corresponding variables in $k[X]$. Then $\mathbb{R}[a_{11}, a_{12}, a_{21}, a_{22}]$ and $\mathbb{R}[a_{11} + ia_{22}, a_{11} - ia_{22}, ia_{12} + a_{21}, ia_{12} - a_{21}]$ defines two different $\mathbb{R}$-structures on X. The first one correspond to the group $SL_2(\mathbb{R})$ and the second one to SU_2.

2.3. **Action of the Galois Group.** Let V be an F-vector space. Let Γ be a group of automorphisms of k such that the fixed points of Γ is $F = \{a \in k \mid \gamma.a = a \ \forall \gamma \in \Gamma\}$. Then Γ acts on $V = k \otimes_F V(F)$ by $\gamma(a \otimes v) = (\gamma.a) \otimes v$. We check that for $a \in F$ and $v, v' \in V$ the action satisfies $\gamma.(av) = a(\gamma.v)$ and $\gamma.(v + v') = \gamma.v + \gamma.v'$, moreover $V(F) = V^\Gamma$, the fix point set.

Proposition 2.3.1. *A subspace W of V is defined over F if and only if $\Gamma.W = W$.*

Proof. Suppose $\Gamma.W = W$. We claim that $W(F) = W^\Gamma$. Clearly $W^\Gamma \subset V^\Gamma = V(F)$. Write $V(F) = W^\Gamma \oplus W'$. We need to show that W^Γ generates W. If not, there exists $0 \neq x \in W$ such that $x = \sum_{i=1}^n a_i x_i$ with $a_i \in k$ and $x_i \in W'$. Suppose x is such an element with minimal expression. Without loss of generality we may assume, $a_1 = 1$. Then for any $\gamma \in \Gamma$, we have $\gamma.x - x = \sum_{i=2}^n (\gamma a_i - a_i) x_i$. From the asumption this is again an element of W contradiction minimality of such an expression in W.

The other part of the proof is obvious. □

Exercise 2.3.2.
(1) Let V and W be two F-vector spaces and let $f \colon V \to W$ be a k-linear map. Then f is defined over F if and only if $f\gamma = \gamma f \ \forall \gamma \in \Gamma$.
(2) Let (a_{ij}) be the matrix of f written with respect to the basis chosen for $V(F)$ and $W(F)$. Show that $\gamma.(a_{ij}) = (\gamma.a_{ij})$, i.e, the action is entrywise. What is the criteria, with such a nice basis, for a map to be defined over F?

Now we assume that k is a Galois extension of F (finite or infinite) and $\Gamma = \mathrm{Gal}(k/F)$. We recall that Γ is a profinite group (i.e., a compact, totally disconnected, topological group) with Krull toplogy. We assume that V is a vector space with discrete topology and Γ acts on it continuously.

Proposition 2.3.3. *With the notation as above, suppose Γ action satisfies $\gamma.(av) = a(\gamma.v)$ and $\gamma.(v + v') = \gamma.v + \gamma.v'$ for $a \in F, v, v' \in V$. Then $V(F) = V^\Gamma$, the fixed points of the action, is an F-structure on V.*

Proof. With the generality about Krull topology, we may assume that V is a finite dimensional vector space and Γ is a finite group corresponding to a finite extension E/F of degree d. We consider $\mathrm{End}_F(k) \cong M_d(F)$. Claim: $\mathrm{End}_F(k) = \{\sum_{\gamma \in \Gamma} c_\gamma \gamma \mid c_\gamma \in k\}$. This follows from strong linear independence of Galois automorphisms and noting that F dimension on both side is d^2. Now, since Γ acts on $V \cong E \otimes_F V(F)$ we use this to get an F-representation of Γ on V, i.e., we get a map $\mathrm{End}_F(k) \to \mathrm{End}_F(V)$. Since $\mathrm{End}_F(k) \cong M_d(F)$ is a simple F-algebra any module has to be direct sum of a simple (unique) module. In this case k is such a module and hence $V \cong k^n$ for some n. In fact, we know that the action is componentwise. This proves that the V^Γ is an F-structure. □

Notice that this gives a one-one correspondance between Γ-action on V (with certain properties) to F-structures on V. The above criterion could be generalised to algebras as well. Let A be a k-algebra with Γ acting on it by ring automorphisms. Then A^Γ is an F-structure on it.

Exercise 2.3.4 (Hilbert 90)**.** Let k/F be a finite Galois extension with $\Gamma = \mathrm{Gal}(k/F)$. Then Γ acts on $GL_n(k)$ entrywise. Let $c\colon \Gamma \to GL_n(k)$ be a map such that $c(\gamma\delta) = c(\gamma)\gamma(c(\delta))$ (1-cocycle). Then there exists $g \in GL_n(k)$ with $c(\gamma) = g^{-1}\gamma(g)$.

Hints: We take $V = k^n$ (with standard basis $\{e_1, \dots, e_n\}$) and define action of Γ satisfying the properties in the above Proposition. Define $\gamma.v = c(\gamma)(\gamma(v))$ where $\gamma(v)$ is the entrywise action of Γ on V. From the Proposition it follows that V^Γ is an F-structure. Let $v_1, v_2, \dots, v_n$ be an F-basis of V^Γ. Take $g \in GL_n(k)$, a matrix which maps v_i to e_i. Then,

$$g^{-1}e_i = v_i = \gamma.v_i = c(\gamma)(\gamma(v_i)) = c(\gamma)\gamma(g^{-1}e_i) = (c(\gamma)\gamma(g^{-1}))(e_i).$$

Hence we get $g^{-1} = c(\gamma)\gamma(g^{-1})$, i.e., $c(\gamma) = g^{-1}\gamma(g)$.

2.4. **Derivations and F-structure.** The set of derivations on k is $Der_F(k) := Der_F(k,k) = \{D\colon k \to k \mid D \text{ is F linear}, D(ab) = aD(b) + D(a)b\}$. It is a k vector space and an F-Lie algebra with $[D,D'] = DD' - D'D$ (bilinearity of $[,]$ is over F only). Let $L \subset Der_F(k,k)$ be a Lie subalgebra such that $F = \{a \in k \mid Da = 0 \forall D \in L\} = Ann(L)$. A **connection** of the F-Lie algebra L which is a k-space on a k-vector space V is a k-linear map $c\colon L \to \mathrm{End}_F(V)$ such that $c(D)(ax) = (Da)x + a(c(D)x)$ for $a \in k, x \in V$. The connection c is called **flat** if c is a Lie algebra homomorphism also.

Now suppose V is an F-space and $\{x_1, \dots, x_n\}$ is a basis of $V(F)$ extended to a basis of V Then there exist a unique flat connection denoted as $c = c_V$ on V which is given by $c(D)(\sum_i a_i x_i) = \sum_i (D.a_i)x_i$ for $a_i \in k, D \in L$.

Proposition 2.4.1. *A subspace W of V is defined over F if and only if $c(L)W \subset W$.*

Corollary 2.4.2. *Let V and W be two F-vector spaces and let $f\colon V \to W$ be a linear map. Then f is defined over F if and only if $fc_V(D) = c_W(D)f \forall D \in L$.*

Exercise 2.4.3. Show that $Der_F(k)$ is a k vector space and an F-Lie algebra with $[D,D'] = DD' - D'D$ (not a k Lie algebra).

Exercise 2.4.4. Prove the Proposition and Corollary above.

Exercise 2.4.5. Show that $Der_F(k)$ is non-trivial in following cases:

1. **transcendental case :** $k = F(x)$ is a transcendental extension of F.
2. **purely inseparable case :** $char(F) = p$ and $k = F(x)/ < x^p - a >$ is a degree p extension with $a \in F$.

The F-Lie subalgebras of $Der_F(k)$ which are k-vector spaces play the similar role in case of transcendental extensions and insperable extensions as Galois group does in the case of separable extensions (see Jacobson, Basic Algebra II, Section 8.15 and 8.16). We will show this in the case of purely inseparable extension below.

2.5. **F-structure over Inseparable Extensions.** Let $char(k) = p > 0$.

Definition 2.5.1 (p-Lie algebra)**.** *A p-Lie algebra L, is a Lie algebra with a map $L \to L$ denoted as $D \mapsto D^{[p]}$ satisfying:*

1. $(aD)^{[p]} = a^p D^{[p]}$
2. $ad(D^{[p]}) = (adD)^p$
3. *Jacobson's Formula:* $(D + D')^{[p]} = D^{[p]} + D'^{[p]} + \sum_{i=1}^{p-1} i^{-1} s_i(D, D')$ *where* $ad(aD + D')^{p-1}(D') = \sum_i s_i(D, D')a^i$.

A p-connection of the p-Lie algebra L on a vector space V is a connection that satisfies, in addition, $c(D^{[p]}) = c(D)^p$.

Example 2.5.2.
1. Let $L = M_n(k)$ be the Lie algebra with $[A, B] = AB - BA$. With the p-operation defined as $A^{[p]} := A^p$, it is a p-Lie algebra.
2. $Der_F(k)$ is a p-Lie algebra with the p-operation $D^{[p]} := D^p$.

Now we take k/F a finite purely inseparable extension such that $k^p \subset F$. We denote by $\mathcal{J} = \mathcal{J}_{k/F}$ the p-Lie algebra of F-derivations of k. With Lie product as commutator and p-operation the ordinary pth power, $\mathcal{J}$ is a p-Lie algebra over F and is a vector space over k. Choose $x_1, \dots, x_d$ in k such that $k = F(x_1, \dots, x_d)$ with minimal such d and $x_i^p = a_i \in F$ $(1 \le i \le d)$.

Lemma 2.5.3. *With notation as above,*

1. $\{x_1^{n_1} \cdots x_d^{n_d} \mid 1 \le n_i < p, 1 \le i \le d\}$ *is a basis of k over F.*
2. *There exists $\partial_i \in \mathcal{J}$ with $\partial_i x_j = \delta_{ij} x_i$. We have $\partial_i^{[p]} = \partial_i, [\partial_i, \partial_j] = 0$ for all $1 \le i, j \le d$.*
3. $\{\partial_i \mid 1 \le i \le d\}$ *is a k-basis of $\mathcal{J}$. We have $[k : F] = p^{\dim_k \mathcal{J}}$.*
4. *The annihilator of $\mathcal{J}$ is F.*

Proof. Suppose the set of elements are dependent. Then we have $k/E/F$ where $k = E(x_1)$ and $E = F(x_2, \dots, x_d)$. The dependence relation implies that $[k : E] < p$ however x_1 satisfies a polynomial of degree p over F. Hence $[k : E]$ must divide some p power hence $[k : E] = 1$, a contradiction. This proves linear dependence.

We do it for one variable first. Let $k = F[T]/ < T^p - a >$. Any derivation on $F[T]$ is given by $\alpha \frac{\partial}{\partial T}$ for $\alpha \in k$. We observe that $T \frac{\partial}{\partial T}$ is a derivation on k.

In general we have $k = F[T_1, \dots, T_d]/ < T_1^p - a_1, \dots, T_d^p - a_d >$. And the derivations $\partial_i = T_i \frac{\partial}{\partial T_i}$ give the space of derivation over k. Notice that this derivation satisfies $\partial_i^p = \partial_i$ (if we take $\partial_i = \frac{\partial}{\partial T_i}$ then it doesn't satisfy this property). □

Proposition 2.5.4. *Let V be a vector space over k with a flat p-connection c of the p-Lie algebra $\mathcal{J}_{k/F}$. Then $V(F) = Ann(\mathcal{J}_{k/F}) = \{x \in V \mid c(D).x = 0 \forall D \in \mathcal{J}_{k/F}\}$ is an F-structure on V.*

Proof. We have a Lie algebra homomorphism $c\colon Der_F(k) \to \mathrm{End}_F(V)$ which is a k-linear map. The elements of the set $\{c(\partial_i)\}$ are $\mathbb{F}_p$-linear maps and form a commutating set (thanks to $[\partial_i, \partial_j] = 0$) of semisimple elements (their action on basis of k/F is such). Hence they can be simultaneously diagonalised and gives following decomposition:

$$V = \bigoplus_{n_1, \dots, n_d} V_{n_1, \dots, n_d}$$

where $V_{n_1, \dots, n_d} = \{x \in V \mid c(\partial_i)x = n_i x, 1 \le i \le d\}$. We claim that $V(F) = V_{0, \dots, 0} = Ann(c)$. This follows from $V_{n_1, \dots, n_d} = x_1^{n_1} \cdots x_d^{n_d} V_{0, \dots, 0}$. □

We further go on to generalise the main theorem of Galois theory for inseparable extensions.

Theorem 2.5.5 (Jacobson)**.** *With notation as above,*

1. *Let $\mathcal{J}_1$ be a p-Lie subalgebra of $\mathcal{J}_{k/F}$, which is a vector space over k. Then $F_1 = Ann(\mathcal{J}_1)$ is a subfield of k containing F and $[k : F_1] = p^{\dim_k \mathcal{J}_1}$.*
2. *This defines a bijection of the set of p-Lie algebras of $\mathcal{J}$ that are k-vector spaces onto the subfields of k containing F. The inverse map is given by $F_1 \mapsto \mathcal{J}_{k/F_1}$.*

Proof. See Basic Algebra volume 2, N. Jacobson, section 8.16, page 533. □

3. Density Criteria for Ground fields

In this section k denotes an algebraically closed field with F a subfield. We denote $\bar{F}$ and F_s for the algebraic closure and separable closure, respectively. Moreover F_s is a Galois extension of F with Galois group Γ. The action of the group Γ can be extended to $\bar{F}$ and the fixed subfield is $F_i = \{x \in \bar{F} \mid x^{p^m} \in F$ for some $m \geq 0\}$, purely inseparable extension. In case of $char = 0$ we have $F_i = F$ and $\bar{F} = (F_i)_s = (F_s)_i$.

3.1. Criteria for a Variety to be defined over F.

Let X be an affine variety over k. Recall that an F-structure on X is equivalent to giving a subalgebra $F[X]$ of $k[X]$ which is k-isomorphic to $k[X]$ after base-change to k.

Lemma 3.1.1. *Let A be an F-algebra. Then there is an affine F-variety X with $A \cong F[X]$ if and only if*

1. *A is of finite type over F.*
2. *For any algebraic extension E of F the algebra $E \otimes_F A$ is reduced.*

Theorem 3.1.2 (Density Theorem)**.** *Let X be an F-variety.*

1. *$X(\bar{F})$ is dense in X. If Y is a closed subvariety of X such that $X(F) \cap Y$ is dense in Y, then Y is defined over F.*
2. *The irreducible components of X are defined over F_s and $X(F_s)$ is dense in X.*

Proposition 3.1.3. (1) *Let Y be a closed subveriety of X. Then Y is defined over F if and only if*

   (a) *Y is defined over F_s,*
   (b) *there is a subset of $Y(F_s)$ that is dense in Y and is stable under the Γ-action on $X(F_s)$.*

(2) *Let Y be an open subvariety of X. The Y is defined over F if and only if*

   (a) *Y is defined over $\bar{F}$,*
   (b) *$Y(\bar{F})$ is a Γ-stable subset of $X(\bar{F})$.*

3.2. Intersection and Fibre defined over F.

Theorem 3.2.1. *Let X be an F-variety and let Y and Z be closed F-subvarieties with a non-empty intersection. Then $Y \cap Z$ is a closed subvariety, which is defined over F if and only if*

1. *F is perfect,*
2. *there is a dense open subset U of $Y \cap Z$ such that for $x \in U$ we have $T_x(Y \cap Z) = T_x(Y) \cap T_x(Z)$.*

Corollary 3.2.2. *Let $\phi \colon X \to Y$ be an F-morphism of irreducible F-varieties. Let $y \in Y(F) \cap Im(\phi)$.*

1. *If F is perfect then the fiber $\phi^{-1}(y)$ is defined over F,*

(2) *Assume that all irreducible components of* $\phi^{-1}(y)$ *have dimension* $\dim X - \dim Y$ *and that in each component* C *of* $\phi^{-1}(y)$ *there exists a simple point* x *such that the tangent map* $d\phi_x \colon T_xC \to T_yY$ *is surjective. Then* $\phi^{-1}(y)$ *is defined over* F.

4. Forms and Cohomology

Here we define commutative cohomology first and then define non-commutative 1-cohomology group. This topic is an important part of the classification of algebraic group which we will see as the workshop progresses. However a warning is on hand that cohomology just keeps track of the forms, it doesn't say anything about its existence.

4.1. **Commutative Cohomology.** Let G be a group and let A be a set on which G acts. We denote $s(a) = {}^s a$ for $s \in G$ and $a \in A$. We call A is a G-set. If A is a group and the action of G is via homomorphisms then we call A is a G-group. Let A be an Abelian G group. We define $\mathcal{C}^0(G, A) = A$ and $\mathcal{C}^i(G, A) = \{a \colon \underbrace{G \times \ldots \times G}_{i} \to A\}$ which is set of all maps from $\underbrace{G \times \ldots \times G}_{i}$ to A. We also write $a(s_1, \ldots, s_i)$ as $a_{s_1,\ldots,s_i}$. We define maps $\delta^0 \colon \mathcal{C}^0 \to \mathcal{C}^1$ by $\delta^0(a)(s) = {}^s a - a$ and

$$\begin{aligned} \delta^i \quad &: \quad \mathcal{C}^i \to \mathcal{C}^{i+1} \\ \delta^i(a)(s_1, \ldots, s_{i+1}) \quad &= \quad {}^{s_1}a(s_2, \ldots, s_{i+1}) \\ &+ \quad \sum_{j=1}^{i} (-1)^j a(s_1, \ldots, s_j s_{j+1}, \ldots, s_{i+1}) + (-1)^{i+1} a(s_1, \ldots, s_i) \end{aligned}$$

Then

$$0 \to \mathcal{C}^0 \xrightarrow{\delta^0} \mathcal{C}^1 \xrightarrow{\delta^1} \mathcal{C}^2 \xrightarrow{\delta^2} \ldots \xrightarrow{\delta^{i-1}} \mathcal{C}^i \xrightarrow{\delta^i} \mathcal{C}^{i+1} \xrightarrow{\delta^{i+1}} \ldots$$

is a chain-complex. Moreover, check that $\delta^{i+1}\delta^i = 0$ for all i. We define $\mathcal{Z}^i(G, A) = ker(\delta^i)$ called cocycles and $\mathcal{B}^i(G, A) = Im(\delta^{i-1})$ called coboundaries. As $\mathcal{B}^i(G, A) \subset \mathcal{Z}^i(G, A)$ we define $H^i(G, A) = \frac{\mathcal{Z}^i(G,A)}{\mathcal{B}^i(G,A)}$ called i-th cohomology group. The cohomology groups are Abelian groups. We write down first few cohomology groups explicitly.

$H^0(G, A)$ **:** Let A be an Abelian G-group. Then $H^0(G, A) = A^G = \{a \in A | {}^s a = a \forall s \in G\}$, set of fixed points of A by the action of G.

$H^1(G, A)$ **:** A map $a : G \to A$ is called a 1-cocycle if

$$a_{st} = a_s + {}^s a_t.$$

For any $c \in A$, define, $a : G \to A$ by $a_s = {}^s c - c$, is a 1-coboundary. We define an equivalence relation on 1-cocycles as follows: two cocycles a, b are related if there exists $c \in A$ such that $b_s = -c + a_s + {}^s c$. The 1-cocycles modulo this equivalence relation form first cohomology group.

$H^2(G, A)$ **:** A map $a : G \times G \to A$ is called a 2-cocycle if

$$a_{s_1 s_2, s_3} = {}^{s_1} a_{s_2, s_3} + a_{s_1, s_2 s_3} - a_{s_1, s_2}.$$

A map $a : G \times G \to A$ such that $a_{s,t} = {}^s b_t - b_{st} + b_s$ for some map $b : G \to A$, is called a 2-coboundary. The quotient group is called 2nd cohomology group.

Remark : Sometimes we will write the commutative group A multiplicatively. We have used here additive notation.

Example 4.1.1. Let E be a finite Galois extension of a field F. Let $G = Gal(E/F)$ be the Galois group. Then G acts on additive group E by evaluation. Then $H^0(G, E) = F$ and $H^i(G, E) = 0$ for all $i \geq 1$. Proof uses "Normal Basis Theorem" and "Shapiro's Lemma".

4.2. **Cohomology and Central Simple Algebras.** Let E be a Galois extension of a field F. Let Γ denote the Galois group $\mathrm{Gal}(E/F)$. Then Γ acts on the Abelian group E^* as follows : $\Gamma \times E^* \to E^*$ given by $(\sigma, \alpha) \mapsto \sigma(\alpha)$. Then,

Proposition 4.2.1. *With above notations, the cohomology groups are :*

1. $H^0(\Gamma, E^*) = F^*$.
2. $H^1(\Gamma, E^*) = \{1\}$ *(Hilbert's Theorem 90).*
3. $H^2(\Gamma, E^*) = \mathrm{Br}(E/F)$.

Proof. To prove $H^1(\Gamma, E^*) = 0$, we let $a\colon \Gamma \to E^*$ is a 1-cocycle. Then $a_{st} = a_s {}^s a_t$ for any $s, t \in \Gamma$. We have to prove that there exists $c \in E^*$ such that $a_s = {}^s c c^{-1}$. We claim that there exists $\alpha \in E^*$ such that $\sum_{\sigma\in\Gamma} a_\sigma \sigma(\alpha) \neq 0$ (follows from lemma below). Put $d = \sum_{\sigma\in\Gamma} a_\sigma \sigma(\alpha)$. Then,

$$s(d) = \sum_{\sigma\in\Gamma} {}^s a_\sigma s\sigma(\alpha) = \sum_{\sigma\in\Gamma} a_s^{-1} a_{s\sigma} s\sigma(\alpha) = a_s^{-1} d.$$

Now we take $c = d^{-1}$ and we get the result.

Lemma 4.2.2. *Let E be a field extension. Let $\{\sigma_1, \ldots, \sigma_n\}$ be distinct field automorphisms of E. Suppose there exists $a_i \in E$ such that $\sum_i a_i\sigma_i(x) = 0$ for all $x \in E$ then $a_i = 0$ for all i.*

To prove last part we need to know the theory of central simple algebras. □

Exercise 4.2.3. Let E/F be a Cyclic (Galois) extension and $\Gamma =< \sigma >$. Let $\alpha \in E^*$ such that $N(\alpha) = 1$. Then there exists $\beta \in E^*$ such that $\alpha = \frac{\beta}{\sigma(\beta)}$.

Let F be a field. Let A be a finite dimensional algebra over F. Then A is called **simple** if it (is a nontrivial semisimple ring and) has no two sided ideals other than $\{0\}$ and A. A finite dimensional algebra is called **central simple** if it is simple and $\mathcal{Z}(A) = F$. From Wedderburn's structure theorem it follows that a central simple algebra A is isomorphic to $M_n(D)$ where D is a central division algebra over F. We define an equivalence relation on the set of finite dimensional central simple algebras over field F as follows. We call A and B, both finite dimensional central simple algebras over field F, are equivalent if any one of the following equivalent conditions are satisfied :

1. If $A \cong M_n(D)$ and $B \cong M_m(D')$ then $D \cong D'$.
2. There exist m, n such that $A \otimes M_m(F) \cong B \otimes M_n(F)$.

The **Brauer group** of a field F is the set of equivalence classes of finite dimensional central simple algebras over F with multiplication defined by tensor product. It is denoted as $\mathrm{Br}(F)$. It is an abelian group. We give few examples here.

1. $\mathrm{Br}(\mathbb{F}_q) = \{0\}$, for any finite field $\mathbb{F}_q$.
2. $\mathrm{Br}(k) = \{0\}$, for any algebraically closed field k. In fact, $\mathrm{Br}(F) = \{0\}$, for any field F of transcendence degree one over an algebraically closed field.
3. $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$.
4. $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$, where $\mathbb{Q}_p$ is the field of p-adic numbers.

Let E/F be a field extension. Then we have a map $\mathrm{Br}(F) \longrightarrow \mathrm{Br}(E)$ defined by $A \mapsto A \otimes E$. The kernel of this map is called **relative Brauer group**, denoted as $\mathrm{Br}(E/F)$. Let A be a central simple algebra. Let $E \subset A$ be a subfield containing F such that $\mathcal{Z}_A(E) = E$, then E is called a **maximal subfield** of A.

Theorem 4.2.4. *Let A be a central simple algebra over field F of dimension n^2. Then any maximal subfield E of A is a splitting field for A, and $[E : F] = [A : E] = n$. Conversely, given* *any finite field extension E of F of degree n, any element of* $\mathrm{Br}(E/F)$ *has a unique representative A of degree n^2 which contains E as a maximal subfield.*

If D is a central division algebra over F of dimension n^2 then there exists a finite Galois extension E of F which is a splitting field for D. Hence

$$\mathrm{Br}(F) = \bigcup_{E} \mathrm{Br}(E/F)$$

where union is taken over all finite Galois extensions of F. Here we determine the structure of any central simple algebra in context of Brauer group.

Lemma 4.2.5. *Let E/F be a Galois extension of fields with Galois group Γ. Let n be the degree of field extension E/F. Let A be a central simple algebra over F containing E as its maximal subfield. Then there exists $x_\sigma \in A, \forall \sigma \in \Gamma$ and $a\colon \Gamma \times \Gamma \to E^*$, a 2-cocycle, such that $A = \oplus_{\sigma\in\Gamma} E x_\sigma$ and the multiplication is given by*

$$\alpha x_\sigma . \beta x_\tau = \alpha\sigma(\beta) a_{\sigma,\tau} x_{\sigma\tau}.$$

Proof. For each $\sigma \in \Gamma$, by Skolem-Noether theorem, there exists $x_\sigma \in A$ such that $x_\sigma a x_\sigma^{-1} = \sigma(a)$ for all $a \in E$. These x_σ's are unique up to a scalar multiplication by elements of E. Moreover, as E is maximal subfield, we get $x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau}$ for some $a_{\sigma,\tau} \in E^*$. This gives a map $a\colon \Gamma\times\Gamma \to E^*$. As the algebra is associative we have $x_\rho(x_\sigma x_\tau) = (x_\rho x_\sigma)x_\tau$ which gives $\rho(a_{\sigma,\tau})a_{\rho,\sigma\tau} = a_{\rho,\sigma}a_{\rho\sigma,\tau}$. Hence a is a 2-cocycle. We know that x_σ's differ by a scalar multiple by elements of E. Suppose $x'_\sigma = f_\sigma x_\sigma$. We get $b_{\sigma,\tau} \in E^*$ such that $b_{\sigma,\tau} x'_{\sigma,\tau} = f_\sigma \sigma(f_\tau) x_\sigma x_\tau$. This gives following relation,

$$b_{\sigma,\tau} f_{\sigma\tau} = f_\sigma \sigma(f_\tau) a_{\sigma,\tau}.$$

Hence the map $c\colon \Gamma \times \Gamma \to E^*$ defined by $c(\sigma,\tau) = \frac{f_\sigma \sigma(f_\tau)}{f_{\sigma\tau}}$ is a 2-coboundary. The maps a and b differ by c. The set $\{x_\sigma\}$ forms a basis for A over E. This defines a map from $\mathrm{Br}(F)$ to $H^2(G, E^*)$. □

Conversely we have,

Lemma 4.2.6. *Let E/F be a Galois extension of fields with Galois group Γ. Let n be the degree of field extension E/F. Let $a\colon \Gamma \times \Gamma \to E^*$ be a 2-cocycle. We put $A = \oplus_{\sigma\in\Gamma} E_\sigma$ and define multiplication as follows :*

$$\alpha x_\sigma . \beta x_\tau = \alpha\sigma(\beta) a_{\sigma,\tau} x_{\sigma\tau}.$$

Then A is a central simple algebra over F containing E as maximal subfield.

The algebra obtained in this lemma is denoted by $[E, \Gamma, a]$. Lemma gives a surjective map form $\mathcal{Z}^2(\Gamma, E^*) \to \mathrm{Br}(E/F)$ defined by $a \mapsto [E, \Gamma, a]$. In fact one can show that the kernel of this map is coboundaries. Hence this proves the remaining part of the proposition. In fact, this map is a group isomorphism.

4.3. **Cohomology and Group Extension.** Let G be a group and A be an abelian group. We will write the group operation in A additively.

Definition 4.3.1. *A group E is called a* **group extension** *of G by A if there is an exact sequence as follows:*

$$1 \to A \xrightarrow{i} E \xrightarrow{\pi} G \to 1.$$

Notice that giving an extension also defines a G-module structure on A as follows: choose $e_g \mapsto g$ (in fact, $e_gA \mapsto g$). Now define $g.a = e_g a e_g^{-1}$ (as A is a normal subgroup of E).

We call two extensions E_1 and E_2 are equivalent if there exists $\beta \colon E_1 \to E_2$, an isomorphism such that following diagram commutes:

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, "Id"] & E_1 \arrow[r] \arrow[d, "\beta"] & G \arrow[r] \arrow[d, "Id"] & 1 \\
1 \arrow[r] & A \arrow[r] & E_2 \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

Verify that two equivalent extensions define isomorphic G-module structure on A.

Now we wish to see how to write all of the group extensions. This we do by using cohomology.

Let E be an extension then we have $G \cong E/A$. Fix a section (equivalent to fixing a quotient representative) $\mu \colon G \to E$ (i.e., $\pi\mu = Id$). Each element of E can be written as $a.\mu(g)$ for some $a \in A$ and $g \in G$. Consider $\mu(g) \in Ag$ and $\mu(h) \in Ah$ as element of E. Then $\mu(g)\mu(h) \in Agh$ hence we can write

$$\mu(g)\mu(h) = f(g,h)\mu(gh)$$

for some $f(g,h) \in A$. This defines a map $f \colon G \times G \to A$ (also called factor sets) which has following properties:

(1) The map f is a 2-cocycle. This is equivalent to associativity of $\mu(g), \mu(h)$ and $\mu(k)$ in A.
(2) Choice of a different section μ' instead of μ gives equivalent cocycles, i.e., f and f' are equivalent.
(3) The extension is split (i.e., section μ is a group homomorphism) if and only if the corresponding cocycle is trivial if and only if $E \cong A \rtimes G$.

This way we show that an extension gives rise to a G-module structure and a 2-cocycle. Next we show the converse.

Let G acts on A and $f \colon G \times G \to A$ be a 2-cocycle. We wish to construct E_f, an extension of G by A. We define $E_f = A \times G$ and

$$(a_1, g).(a_2, h) = (a_1 + g.a_2 + f(g,h), gh).$$

Then $(f(1,1),1)$ is the identity element and $(a,x)^{-1} = (-x^{-1}.a - f(x^{-1},x) - f(1,1), x^{-1})$.

Theorem 4.3.2. *Let G be a group and A an abelian group. Then the set of all group extensions of G by A, i.e., $Ext(G,A)$, is in bijection with $H^2(G,A)$.*

4.4. **Non-Commutative Cohomology.** Let G be a (profinite) group and A be a set (with discrete topology) on which G acts (continuously). We denote $s(a) = {}^sa$ for $s \in G$ and $a \in A$. We call A, a G-set. If A is a group and the action of G is via homomorphisms then we call A, a G-group. We define cohomology groups as follows.

$H^0(G,A)$ **:** Let A be a G-set. Then $H^0(G,A) = A^G = \{a \in A \mid {}^sa = a \forall s \in G\}$, set of fixed points of A by the action of G.

$H^1(G,A)$ **:** Let A be a G-group. A map $a : G \to A$ is called a 1-cocycle if

$$a_{st} = a_s{}^s a_t.$$

Two 1-cocycles a, b are equivalent if there exists $c \in A$ such that $b_s = c^{-1} a_s{}^s c$. This is an equivalence relation on the set of 1-cocycles and the quotient group is $H^1(G,A)$. The set $H^1(G,A)$ need not be group in general but it always has a distinguished element namely the class of 1-cocycles of the form $b^{-1s}b$ for $b \in A$.

If A is a commutative group we can define higher cohomology groups as we did in the last section 4.1.

Proposition 4.4.1 (Hilbert 90). *Let E be a finite Galois extension of F with Galois group Γ. Let Γ acts on the group $GL_n(E)$ entrywise. Then $H^0(\Gamma, GL_n(E)) = GL_n(F)$ and $H^1(\Gamma, GL_n(E)) = \{1\}$.*

Proof : Let $a\colon \Gamma \to GL_n(E)$ be a 1-cocycle. If we take $d = \sum_{\sigma\in\Gamma} a_\sigma \sigma(A)$ for some $A \in M_n(E)$. Then $s(d) = a_s^{-1}d$. If we can get d invertible, we will be done. Put $b = \sum_{\sigma\in\Gamma} a_\sigma\sigma$ and consider W a subspace generated by $\{b(x) | x \in E^n\}$. Then $W = E^n$. For $f \in E^{n*}$ suppose we have $f(b(x)) = 0$ for all $x \in E^n$. Then $0 = f(b(\lambda x)) = \sum_{\sigma\in\Gamma} f(a_\sigma\sigma(\lambda x)) = \sum_{\sigma\in\Gamma} f(a_\sigma\sigma(x))\sigma(\lambda)$ for all $\lambda \in E$. But this gives $f(a_\sigma\sigma(x)) = 0$ for all $x \in E^n$. Hence $f = 0$. This proves that $W = E^n$.

Choose $\{x_1, \ldots, x_n\} \subset E^n$ such that $y_i = b(x_i)$ are linearly independent. Let A be the matrix with columns $\{x_1, \ldots, x_n\}$ then $b = (b(x_1), \ldots, b(x_n)) = (y_1, \ldots, y_n)$ is the required invertible matrix. □

Example 4.4.2 (Kummer Theory). Let n be an integer coprime to the characteristic of k, and assume that k contains the group μ_n of the n-th roots of unity. Let K be the separable closure of k. Then we have the short exact sequence of G-groups

$$\{1\} \longrightarrow \mu_n \longrightarrow K^* \xrightarrow{u} K^* \longrightarrow \{1\}$$

with $u(x) = x^n$. This gives rise to a long cohomology sequence and $H^1(G, K^*) = \{1\}$ implies that $H^1(G, \mu_n) = k^*/k^{*n}$. Considering $H^1(G, \mu_n)$ corresponds to looking at cyclic extensions of k with Galois group $\mathbb{Z}/n\mathbb{Z}$. Any element $a \in k^*$ such that $a \notin k^{*n}$ defines such a field extension by taking splitting field of the polynomial $X^n - a$. And this is the only way to get such an extension.

4.5. **Forms.** Let X be an F-variety and E a subfield of k containing F.

Definition 4.5.1. *An E-form of X is an F-variety Y which is E isomorphic to X, i.e., $X(E) \cong_E Y(E)$.*

We denote by $\Phi(E/F, X)$ the set of F-isomorphism classes of E-forms of X, i.e.

$$\Phi(E/F, X) = \{Y \mid Y \text{ an } F-\text{variety }, X(E) \cong_E Y(E)\}.$$

We will take E/F a Galois extension. Let $\Gamma = Gal(E/F)$ and moreover assume that X be an affine F-variety. The group Γ acts on $E[X] = E \otimes F[X]$ as ring automorphism where action is given by $\gamma.(a \otimes v) = \gamma(a) \otimes v$. This action is continuous relative to Krull topology on Γ and discrete topology on $E[X]$. Let $A := \mathrm{Aut}_E(X) = \mathrm{Aut}_{E-alg}E[X]$ (the algebra automorphisms of $E[X]$ can be thought of variety automorphisms of X over E). Then Γ acts on A continuously as $\gamma.\phi = \gamma\phi\gamma^{-1}$.

Theorem 4.5.2. *We assume E/F is a Galois extension and X an affine F-variety. There is a bijection $\Phi(E/F, X) \to H^1(\Gamma, \mathrm{Aut}_E(X))$ such that the class of X corresponds to* 1.

Proof. We follow the conventions defined above. First we wish to define the map which gives the above bijection. Let Y be an E-form of X, i.e., there exists an E-isomorphism $\phi\colon E[Y] \to E[X]$. Using this we define $c := c_\phi\colon \Gamma \to A$ by $c(\gamma) = \phi\gamma\phi^{-1}\gamma^{-1}$. Since

$$c(\gamma\delta) = \phi\gamma\delta\phi^{-1}(\gamma\delta)^{-1} = \phi\gamma(\phi^{-1}\gamma^{-1}\gamma\phi)\delta\phi^{-1}\delta^{-1}\gamma^{-1} = (\phi\gamma\phi^{-1}\gamma^{-1})\gamma.(\phi\delta) = c(\gamma)\gamma.c(\delta).$$

This defines a map $\Phi(E/F, X) \to \mathscr{Z}^1(\Gamma, \mathrm{Aut}_E(X)) \to H^1(\Gamma, \mathrm{Aut}_E(X))$ by $\phi \mapsto c_\phi$. We need to check whether this map is well defined, i.e., it doesn't depend on the isomorphism ϕ. Suppose

$\phi, \phi' \colon E[Y] \to E[X]$ are E-isomorphisms. Then we claim that c_ϕ and $c_{\phi'}$ are equivalent cocycles. We check this:

$$c_\phi(\gamma) = \phi\gamma\phi^{-1}\gamma^{-1} = \phi(\phi'^{-1}\phi')\gamma(\phi'^{-1}\gamma^{-1}\gamma\phi')\phi^{-1}\gamma^{-1} = (\phi'\phi^{-1})^{-1}c_{\phi'}(\gamma)\gamma.(\phi'\phi^{-1}).$$

Now we show that the map is injective. Let Y and Z be two E-forms of X, i.e., there exists E-isomorphisms $\phi\colon E[Y] \to E[X]$ and $\psi\colon E[Z] \to E[X]$. Suppose the respective cocycles $c = c_\phi, d = c_\psi$ are equivalent, i.e., there exists $a \in \mathrm{Aut}_E(X)$ such that $d(\gamma) = a^{-1}c(\gamma)\gamma.a \forall \gamma \in \Gamma$. Then we claim that $E[y]$ and $E[Z]$ are F-equivalent. For this we note that:

$$a\psi\gamma\psi_{-1}\gamma^{-1} = ad(\gamma) = c(\gamma)\gamma.a = \phi\gamma\phi^{-1}\gamma^{-1}\gamma a\gamma^{-1}$$

which gives $\phi^{-1}a\psi\gamma = \gamma\phi^{-1}a\psi$. Hence the map $\phi^{-1}a\psi$ is an isomorphism of $E[Z]$ to $E[Y]$ defined over F, i.e., Y and Z are F-isomorphic forms of X.

Now we need to prove that the map is surjective. Let $c\colon \Gamma \to \mathrm{Aut}_E(X)$ be a 1-cocycle. We define an action of Γ on $E[X]$ using this cocycle as follows: $(\gamma, a) \mapsto c * \gamma = c(\gamma)\gamma.a$. This action satisfies the property of the Proposition 2.3.3 hence $E[X]^\Gamma$ is an F-structure which we denote by $F[X]_c$ (the corresponding variety X_c is said to be obtained from X by twisting with cocycle c). This gives the required F-form. □

Next we give some applications of this theorem.

Exercise 4.5.3. Let E/F be a Galois extension with group Γ.

(1) $H^1(\Gamma, GL_n(E)) = 1$.
(2) $H^1(\Gamma, Sp_{2n}(E)) = 1$.
(3) For $char(k) \neq 2$, $H^1(\Gamma, O_n(E))$ is in one-one correspondence with non-degenerate symmetric bilinear forms on F^n that are E-isomorphic.
(4) $H^1(\Gamma, E)$ is trivial.

Example 4.5.4 (Classical Groups)**.** Central simple algebras with involutions have automorphism groups as classical groups. Also most of the classical groups have there automorphism group as themselves. The theorem above implies that the central simple algebras with involutions over field F ($char(F) \neq 2$) are in one-one correspondence with F-forms of classical groups (with few exceptions).

Example 4.5.5 (Groups of type G_2)**.** Octonion algebras over field F are in one-one correspondence with the forms of groups of type G_2 over F.

5. Restriction of the Ground Field

5.1. **What do we want!** Let E/F be a field extension of degree n. We have **base change** functor $E\otimes_F$ defined from category of F algebras to category of E algebras by $B \mapsto E \otimes_F B$. Let us fix an E-algebra A. Then $Sp_E(A)$ is an affine E-functor. This gives us an F-functor $Sp_F(A)$ defined by $Sp_F(A)(B) := Sp_E(A)(E \otimes_F B) = \mathrm{Hom}_{E-alg}(A, E \otimes_F B)$. Now the question is whether this F-functor is representable, i.e., does there exists RA an F-algebra such that $Sp_F(A)(B) = Hom_{F-alg}(RA, B)$. In that case RA is adjoint to $E\otimes_F$. The next construction answers this question.

We explain the above problem in the language of affine variety. Let X be an affine variety defined over E. Does there exists an F variety RX such that $RX(F) = X(E)$? This way we reduce the questions about X to a variety defined over F, though the variety RX itself may be more complicated.

Example 5.1.1. Let $\mathbb{A}^m$ be affine m-space over E. Then $R\mathbb{A}^m = \mathbb{A}^{mn}$. Intuitively for each basis vector we replace it with n independent basis vectors.

Example 5.1.2. Let us take field extension $\mathbb{C}/\mathbb{R}$ and the variety $G_m(\mathbb{C}) = \mathbb{C}^*$ given by $XY = 1$. To obtain $\mathbb{R}G_m$ we substitute $X = X_1 + iX_2$ and $Y = Y_1 + iY_2$. And the equation $XY = 1$ gives us $X_1Y_1 - X_2Y_2 = 1$ and $X_1Y_2 + X_2Y_1 = 0$. Hence $\mathbb{R}G_m$ is the variety given by zeros of these two equations in $\mathbb{R}^4$. Observe that as a set it is just $\mathbb{C}^*$.

Exercise 5.1.3 (A silly doubt!)**.** Does $RA = A$ works?

5.2. **Existence of Restriction.** Let E/F be field extension of degree n. We fix an F-bilinear pairing $<,>$ between F-vector spaces E and E' (dual of E). We fix $\{x_1, \dots, x_n\}$ as an F-basis of the vector space E and $\{x'_1, \dots, x'_n\}$ that for E. Let A be an E-algebra. Denote $S = sym_F(E' \otimes_F A)$, the symmetric algebra. Let I be an ideal of S generated by elements:

$$x' \otimes ab = \sum_{i,j} < x_ix_j, x' > (x'_i \otimes a)(x'_j \otimes b) \quad \text{and} \quad x' \otimes x =< x, x' >$$

where $x \in E, x' \in E'$ and $a, b \in A$. If $I \neq S$ we say that restriction of A over F exists and denote the F-algebra $RA = R_{E/F}A = S/I$. The algebra RA satisfies certain universal property if it exists.

Proposition 5.2.1 (Universal Property of RA)**.** *With notation as above, suppose RA exists. Then,*

1. *There exists an E-homomorphism $\rho\colon A \to E \otimes_F RA$ such that the pair (RA, ρ) satisfies following universal property: for any pair (B, σ) with B an F-algebra and $\sigma\colon A \to E \otimes_F B$ and E-homomorphism there exists a unique F-homomorphism $\tau\colon RA \to B$ such that $\sigma = (1 \otimes \tau)\rho$.*
2. *Suppose there exists an F-algebra B with an E-homomorphism $\sigma\colon A \to E \otimes_F B$ then the restriction of A exists.*

Proof. We first define an F-bilinear map $u\colon E' \times A \to RA$ by $(x', a) \mapsto x' \otimes a$. This amounts to looking at the F-linear map $E' \otimes_F A \to sym_F(E' \otimes_F A) \to RA$. Moreover u satisfies following:

$$u(x', ab) = \sum_{i,j} < x_ix_j, x' > u(x'_i, a)u(x'_j, b) \quad \text{and} \quad u(x', x) =< x, x' >$$

where $x \in E$. Now using this we define the map $\rho\colon A \to E \otimes_F RA$ as follows:

$$\rho(a) = \sum_i x_i \otimes u(x'_i, a).$$

The above properties of u are equivalent to saying ρ is an E-homomorphism.

Now let (B, σ) be the F-algebra with E-homomorphism $\sigma\colon A \to E \otimes_F B$. We define F-linear maps $\sigma_i\colon A \to B$ such that

$$\sigma(a) = \sum_i x_i \otimes \sigma_i(a).$$

Then σ_i satisfies the following relations:

$$\sigma_i(ab) = \sum_{r,s} < x_rx_s, x'_i > \sigma_r(a)\sigma_s(b) \quad \text{and} \quad \sigma_i(x) =< x, x'_i >$$

which reflects the relations for u. Now to define a map $\tau\colon RA \to B$ first we define a map $\bar{\tau}\colon S \to B$ by $x'_i \otimes a \mapsto \sigma_i(a)$. Verify that I is contained in the kernel of this map hence we get the required map τ.

For the proof of second part, suppose we have such a B and an homomorphism σ. Then we can define a map from $S \to B$ as above whose kernel contains I. Hence $I \neq S$ and RA exists. □

Exercise 5.2.2. Show that the map ρ defined in the proof of the proposition above is an E-algebra homomorphism.

Corollary 5.2.3. *The universal property is equivalent to the following map being bijection:*

$$\mathrm{Hom}_{E-alg}(A, E \otimes_F B) \to \mathrm{Hom}_{F-alg}(R_{E/F}A, B).$$

This corollary can also be expressed as $A(E \otimes_F B) = RA(B)$. If we take $B = k$ we get $RA(k) = A(E \otimes_F k) \cong A(k^n)$ which gives support to our intuitive idea for substituting n-variables for a variable of A to get RA points.

Corollary 5.2.4. *The restriction RA exists if one of the following holds:*

(1) *there exists an E-homomorphism $A \to E$.*
(2) *A is an affine E-algebra.*

Proof. In first case we take $B = F$ and σ as the given map. □

Example 5.2.5 (RA need not exist)**.** Let $char(F) = p > 0$ and $E = F(x)$ with $x^p \in F$ be degree p extension. Consider E-algebra $A = E(a) = E(x^{\frac{1}{p}})$ where $a^p = x$. Suppose we have (B, σ) with and E-homomorphism $\sigma\colon A \to E \otimes_F B$. Suppose $\sigma(a) = \sum_i x_i \otimes b_i$. Then $\sigma(a^p) = (\sigma(a))^p = 1 \otimes \sum_i x_i^p b_i^p$, on other hand, $\sigma(a^p) = \sigma(x) = x(1 \otimes 1) = x \otimes 1$. This implies $x \otimes 1 = 1 \otimes \sum_i x_i^p b_i^p$, a contradiction.

Example 5.2.6. Let $A = E[T]$. We claim that $RA = sym_F(E')$ and the map ρ is given by $T \mapsto \sum_i x_i \otimes x'_i$. For this we follow the construction and observe that $x' \otimes xT = \sum_{i,j} < x_i x_j, x' > (x'_i \otimes x)(x'_j \otimes T)$ where $x'_i \otimes x \in F$. We define the map $RA \to sym(E')$ by $x'_i \otimes T \mapsto x'_i$.

In above example we can also do following: $RA(k) = A(E \otimes_F k) = \mathrm{Hom}_{E-alg}(E[T], E \otimes_F k)$. Any such homomorphism is defined by $T \mapsto \sum_i x_i \otimes \alpha_i = (\alpha_1, \ldots, \alpha_n)$.

5.3. **Restriction of Ground Field for a Variety.** Let $A = E[X]$ be an affine E-algebra. Then RA exists and is an F-algebra of finite type. But RA need not be an affine F-algebra. We consider two special cases in more detail:

a. E is separable over F.
b. $p = char(F) > 0$ and $E = F(x)$ with $x^p \in F$.

Let us look at separable case first. Let $\bar{F}$ be the separable closure of F in k. Denote by $\Sigma = \{\sigma \mid \sigma\colon E \to \bar{F}, F\text{-isomorphism}\}$. We denote the field containing all σE by $\tilde{E}$ (in case it's Galois extension $\tilde{E} = E$). For $\sigma \in \Sigma$ we define an E-algebra structure on $\tilde{E}$ denoted by $\tilde{E}_\sigma$ as $E \times \tilde{E}_\sigma \to \tilde{E}_\sigma$ given by $(x, y) \mapsto \sigma(x)y$ (note that $\tilde{E}_1$ is usual $\tilde{E}$). Now we take E-algebra

$$B_\sigma = \tilde{E}_\sigma \otimes_E A.$$

Proposition 5.3.1. *There is an isomorphism*

$$\alpha\colon \tilde{E} \otimes_F RA \to \otimes_{\tilde{E}, \sigma \in \Sigma} B_\sigma$$

such that $\alpha(1 \otimes \rho)$ is the canonical injection of B_1 into the tensor product.

Proof. To define the isomorphism we first write a set of generators for $\tilde{E} \otimes_F RA$. We take elements $\tilde{u}(\sigma, a) = \sum_i \sigma(x_i) \otimes u(x'_i, a) \in \bar{F} \otimes_F RA$ for $\sigma \in \Sigma$ and $a \in A$. We claim that

$\tilde{u}(\sigma, ab) = \tilde{u}(\sigma, a)\tilde{u}(\sigma, b)$ and $\tilde{u}(\sigma, x) = \sigma(x) \otimes 1$ and the set $\{\tilde{u}(\sigma, a) \mid \sigma \in \Sigma, a \in A\}$ generates $\tilde{E} \otimes_F RA$.

Now we define the map α be $\tilde{u}(\sigma, a) \mapsto \bigotimes_i (\sigma x_i \otimes a)$. □

Corollary 5.3.2. *If E/F is separable then any E-algebra admits restriction of the ground field.*

The second case of inseparable extension involves considerable amount of analysis. Interested reader may look at the book. Finally we come to the main theorem.

Theorem 5.3.3. (1) *Let X be an irreducible, smooth, affine E-variety. There exists an irreducible, smooth, affine F-variety $\prod X$ or $\prod_{E/F} X$, together with a surjective E-morphism $\pi\colon \prod X \to X$ such that the following universal property holds for $(\prod X, \pi)$: for any (Y, ϕ), Y an affine F-variety with E-morphism $\phi\colon Y \to X$ there exists a unique F-morphism $\psi\colon Y \to \prod X$ with $\phi = \pi\psi$. Moreover, the pair $(\prod X, \pi)$ is unique up to isomorphism.*

(2) *If E/F is separable then smoothness and irreducibility may be omitted from assumption and conclusion both.*

Corollary 5.3.4. $\dim \prod_{E/F} X = [E : F] \dim X$.

References

[Bo] A. Borel, *"Linear algebraic groups"*, Second edition. Graduate Texts in Mathematics, 126. Springer-Verlag, New York, 1991.

[DF] Dummit, Foote, *"Abstract Algebra"*.

[FD] B. Farb; R. K. Dennis, *"Noncommutative algebra"*, Graduate Texts in Mathematics, 144. Springer-Verlag, New York, 1993.

[Hu] J. E. Humphreys, *"Linear algebraic groups"*, Graduate Texts in Mathematics, No. 21. Springer-Verlag, New York-Heidelberg, 1975.

[Ja] J. C. Jantzen, *"Representations of algebraic groups"*, Second edition. Mathematical Surveys and Monographs, 107. American Mathematical Society, Providence, RI, 2003.

[K] M. Kneser, *"Lectures on Galois Cohomology of Classical Groups"*, Tata lecture notes, 47 (1969).

[NSW] Neukirch, Schmidt, Wingberg, *"Cohomology of Number Fields"*.

[PR] V. Platonov; A. Rapinchuk, *"Algebraic groups and number theory"* Translated from the 1991 Russian original by Rachel Rowen. Pure and Applied Mathematics, 139. Academic Press, Inc., Boston, MA, 1994.

[Se] J. P. Serre, *"Galois cohomology"*, Springer-Verlag, Berlin, (1997).

[Sp] T. A. Springer, *"Linear algebraic groups"*, Second edition. Progress in Mathematics, 9. Birkhuser Boston, Inc., Boston, MA, 1998.

The Institute of Mathematical Sciences, C.I.T. Campus Taramani, Chennai 600113 INDIA
E-mail address: anupamk18@gmail.com