1 Descent data

Definition 1. A homomorphism of commutative rings $A \to B$ is called *faithfully flat* if B is flat as an A-module and $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective.

Theorem 2. *A homomorphism of commutative rings $A \to B$ is faithfully flat if and only if a sequence of A-modules* (1)

$$M' \to M \to M'', \tag{1}$$

is exact if and only if the induced sequence of B-modules (2)

$$B \otimes_A M' \to B \otimes_A M \to B \otimes_A M'' \tag{2}$$

is exact.

Let B be an A-algebra. Set $B_0 = B$ and $B_n = B \otimes_A B_{n-1}$ for all integers $n \geq 1$. If $[n] = \{0, 1, \ldots, n\}$ denotes a finite set with $n+1$ elements then any function $[n] \to [m]$ induces an A-algebra homomorphism $B_n \to B_m$.

Definition 3. A *descent datum* for B over A consists of B_n-modules M_n for every integer $n \geq 0$ and homomorphisms $M_n \to M_m$ for every function $[n] \to [m]$ such that the induced maps (3)

$$B_m \otimes_{B_n} M_n \to M_m \tag{3}$$

are isomorphisms. The descent datum is denoted $M_\bullet$.

A morphism of descent data from $M_\bullet$ to $N_\bullet$ consists of homomorphisms of B_n-modules $M_n \to N_n$ for every $n \geq 0$ such that the diagrams (**??**) commute:

$$\begin{tikzcd} M_n \arrow[r] \arrow[d] & M_m \arrow[d] \\ N_n \arrow[r] & N_m \end{tikzcd}$$

The category of descent data is denoted $B_\bullet$-Mod.

Lemma 4. *(i) Any descent datum $M_\bullet$ for B over A is determined up to unique isomorphism by M_0 and M_1 and the homomorphisms between them.*

(ii) Once M_0, M_1, and M_2 have been specified, along with the maps between them, there is a unique way of extending them to a descent datum for B over A.

Lemma 5. *Suppose that M is an A-module. For each n, set $M_n = B_n \otimes_A M$. Then $M_\bullet$ is a descent datum. This determines a functor:*

$$\Phi : A\text{-}\mathbf{Mod} \to B_\bullet\text{-}\mathbf{Mod} : M \mapsto B_\bullet \otimes_A M \tag{4}$$

Lemma 6. *Suppose that $M_\bullet$ is a descent datum. Let v_0 and v_1 denote the two maps $M_0 \to M_1$ and set $M = \ker(v_0 - v_1)$. Then M is an A-module. This determines a functor:*

$$\Psi : B_\bullet\text{-}\mathbf{Mod} \to A\text{-}\mathbf{Mod} : M_\bullet \mapsto \ker(v_0 - v_1) \tag{5}$$

Lemma 7. *Suppose that there is a homomorphism of A-algebras $B \to A$. Then A-**Mod** and B-**Mod** are equivalent.*

Theorem 8. *Let B be a faithfully flat A-algebra. Then the category of descent data for B over A is equivalent to the category of A-modules.*

Lemma 9. *Every field extension is faithfully flat.*

2 Galois theory

Suppose that K is a field and L is an extension of K. Define $L_\bullet$ and $L_\bullet$-**Mod** as in the last section.

Definition 10. Let A be a commutative ring. A A-algebra B is said to be *split* if it is isomorphic to a finite product of copies of A.

If K is a field and L is a finite extension of K then L is called *separable* if there is a field extension $\overline{K} \supset K$ such that $L \otimes_K \overline{K}$ is a split $\overline{K}$-algebra. The field $\overline{K}$ is called a *splitting field* of L.

A finite field extension $L \supset K$ is said to be *Galois* if it is separable and is a splitting field for itself.

Lemma 11. *Let L be a finite extension of a field K. Then $\overline{K} \supset K$ is a splitting field for L if and only if the minimal polynomial of each element of L splits into distinct linear factors over K.*

Lemma 12. *Let L be a finite Galois extension of K. The set of K-algebra homomorphisms from L to itself is a group, called the* Galois group *of L over K.*

Suppose that L is a Galois extension of K with Galois group G. Let A be a K-algebra. The set $X = \mathrm{Hom}_K(A, L)$ of K-algebra homomorphisms from A to L has an action of G, by $g.f(x) = g(f(x))$ for all $g \in G$, all $f \in X$, and all $x \in A$.

Theorem 13 (Galois theory)**.** *There is a contravariant equivalence of categories between L-split finite K-algebras and G-sets sending a K-algebra A to $\mathrm{Hom}_K(A, L)$.*

The goal of this section is to prove this theorem using faithfully flat descent. First we should see how it implies the usual statement of Galois theory:

Lemma 14. *Under the equivalence of Theorem 13, the K-algebra K corresponds to the trivial action of G on a 1-point set. The K-algebra L corresponds to the action of G on itself.*

Corollary 14.1. *Still using the notation of Theorem 13, the intermediate fields of $K \subset L$ correspond to the transitive G-sets, which correspond to the subgroups of G.*

2.1 Split algebras and sets

Notation 15. If A is a ring and X is a set, A^X denotes the ring of functions from X to A.

Lemma 16. *Let K be a field and let L be a split K-algebra. Let X be the set of K-algebra homomorphisms from L to K. Then there is a natural isomorphism*

$$L \xrightarrow{\sim} K^X$$

Corollary 16.1. *The category of split K-algebras is contravariantly equivalent to the category of sets.*

Corollary 16.2. *Let K be a field and let L be a separable K-algebra. Let $\overline{K}$ be a splitting field of L. Then there is a natural isomorphism*

$$L \otimes_K \overline{K} \xrightarrow{\sim} \overline{K}^X.$$

Corollary 16.3. *If K is a field and L is a Galois extension of K. Then there is a natural isomorphism*

$$L \otimes_K L \xrightarrow{\sim} L^G$$

where G is the group of K-automorphisms of L.

The action of $G \times G$ on $L \otimes_K L$ by $(g, h).(x \otimes y) = (g.x) \otimes (g.y)$ goes over to the action sending $(x_t)_{t \in G}$ to $(h.x_{tg^{-1}})_{t \in G}$.

Likewise, there is a natural isomorphism

$$L \otimes_K L \otimes_K L \simeq L^{G \times G}.$$

Definition 17. Let L be a Galois extension of K, with Galois group G. A G-L vector space is an L-vector space V with a linear action of G intertwining the action on L. That is:

(i) For all $g \in G$, all $\lambda \in L$, and all $x \in V$ we have $g.(\lambda x) = (g.\lambda)(g.x)$.

(ii) For all $g \in G$ and all $x, y \in V$, we have $g.(x + y) = g.x + g.y$.

A *(commutative) G-L-algebra* is a G-L-vector space A together with a G-L-vector space homomorphism $\mu : A \otimes_L A \to A$ that makes A into a commutative ring.

A finite dimensional G-L-algebra is *L-split* if its underlying L-algebra is split.

Lemma 18. *The category of L-split G-L-algebras is anti-equivalent to the category of G-sets.*

2.2 Galois descent

For the whole section, K is a field and L is a Galois extension of K with Galois group G.

Lemma 19. *The category of descent data, $L_\bullet$-**Mod**, is equivalent to the category G-L vector spaces.*

Corollary 19.1. *The category of G-L-vector spaces is equivalent to the category of K-vector spaces. The inverse equivalences send a K-vector space V to $L \otimes_K V$ and a G-L vector space W to its G-invariant subspace W^G.*

Corollary 19.2. *The category of K-algebras is equivalent to the category of G-L-algebras.*

Corollary 19.3. *The category of L-split K-algebras is equivalent to the category of L-split G-L-algebras, which is equivalent to the category of G-sets.*

Corollary 19.4. *There is a one-to-one correspondence between the K-subalgebras of L, the L-split G-L-subalgebras of L^G, and the subgroups of G.*