DESCENT THEORY: FROM GENERAL TO SPECIAL

CORNELIUS GREITHER

1. The basic idea of a descent datum

All rings are assumed commutative. Let $R \subset S$ be an extension of rings; $\otimes$ stands for $\otimes_R$, and ${}_SM$ is short for $S \otimes M$. The question is: When an S-module N is given, how can we decide whether N has the form ${}_SM$ for some R-module M, and can we describe the candidates M? If $N = {}_SM$, then there is an isomorphism $g : S \otimes {}_SM \to {}_SM \otimes S$, sending $s \otimes t \otimes m$ to $s \otimes m \otimes t$, in other words: just left-shifting the M-entry. Then g has two properties. First it makes the following diagram commute:

$$\begin{tikzcd}
 & & S \otimes {}_SM \arrow[dd, "g"] \\
M \arrow[r] \arrow[urr, bend left] \arrow[drr, bend right] & {}_SM \arrow[ur, "1\otimes -"] \arrow[dr, "-\otimes 1"'] & \\
 & & {}_SM \otimes S
\end{tikzcd}$$

For the second property we need shorthand notation. The map $g_1 : S \otimes S \otimes {}_SM \to S \otimes {}_SM \otimes S$ arises from g via tensoring with S on the left; similarly g_3 by tensoring on the right, and g_2 by tensoring in the middle. All these maps are simple to imagine, but g_2 is the most awkward to write down: if $h : S \otimes {}_SM \to {}_SM \otimes S$ is any map and $h(s \otimes n) = \sum_i n_i \otimes s_i$, then $h_2(s \otimes t \otimes n) = \sum_i n_i \otimes t \otimes s_i$. The second property of g is then

$$g_2 = g_3 \circ g_1.$$

The effect of either side in this equation is simply shifting M from right to left; in one go if we use g_2, and in two moves, via the middle, if we use $g_3 g_1$. The idea is now to recover M as the difference kernel of

$$\begin{tikzcd}
{}_SM \arrow[r, shift left, "g\circ(1\otimes -)"] \arrow[r, shift right, "-\otimes 1"'] & {}_SM \otimes S
\end{tikzcd} \quad .$$

A minimal requirement for this to work is that the functor $M \mapsto {}_SM$ is exact, in other words, S/R should be flat. Moreover it should work in the simplest of all cases, that is, R should identify with the kernel of the map $S \to S \otimes S$, $s \mapsto 1 \otimes s - s \otimes 1$. This excludes a lot of otherwise nice extensions S/R. For instance when R is a domain and

S any localization of R within $\mathrm{Quot}(R)$, then $S \otimes S$ identifies with S and the map $s \mapsto 1 \otimes s - s \otimes 1$ is the zero map, so the kernel is S, hence too large.

The correct condition for the most general version of descent is that S/R should be *faithfully* flat. A convenient definition of this is: S is flat over R and for all $\mathfrak{m}$ in $\mathrm{Max}(R)$, $\mathfrak{m}S$ is a proper ideal of S. A very useful characterization is: The functor $M \mapsto {}_SM$ preserves, and detects, exactness. We are now ready for the basic concept.

Definition: A *descent datum* is given by an S-module N and an $S\otimes S$-linear isomorphism $g : S \otimes N \to N \otimes S$ such that $g_2 = g_3 g_1$. Descent data form a category, when we declare: A morphism of descent data (N, g) and (N', g') is an S-linear map $f : N \to N'$ making the obvious square commute (that is, $g' f_1 = f_2 g$).

We have described above a functor J from Mod-R into the category of descent data: M goes to $N = {}_SM$, and g was defined explicitly. The basic result, which is not very hard to prove, says that *this functor J is an equivalence of categories.* The inverse functor, on the level of modules, is given by taking a difference kernel similarly as above. Everything works fine if we impose extra structure on modules. The cases we are interested in are mainly R-algebras and R-Hopf algebras. Then all occurring morphisms, like g and f in the above definition, are of course required to also be in the relevant category.

2. Twisted forms and Amitsur cohomology

We take a new point of view now. Let us start with $N = {}_SM$, where the R-module M is given, and look for other modules M' obtained by descent data of the form (N, g). In other words, we try to solve the "equation"

$$S \otimes_R M' \cong S \otimes_R M$$

for M'. If the "equation" holds, M' is called an *S-form* of M.

We now identify $S \otimes {}_SM$ and ${}_SM \otimes S$ with ${}_{S\otimes S}M$, the module M base-changed from R to $S \otimes S$. (One identification is obvious, the other just shifts elements of M.) This allows us to simply consider the map g in a descent datum for $N = {}_SM$ as an automorphism of ${}_{S\otimes S}M$. We need to restate the descent condition. For $i = 1, 2, 3$, let $a_i : S\otimes S \to S\otimes S\otimes S$ be the map that inserts 1 at position i. Then g_i identifies with the map $a_{i*}g$ (the basechanged map along the inclusion of rings given by a_i). The descent condition is still

$$g_2 = g_3 \circ g_1 \in \mathrm{Aut}_{S\otimes S\otimes S}\,({}_{S\otimes S\otimes S}M).$$

Every isomorphism g satisfying this condition defines a form M_g, and one can show that $M_g \cong M_h$ iff there is $f \in \mathrm{Aut}_S({}_SM)$ such that

$$h = f_2 \circ g \circ f_1^{-1}.$$

For each n, we have $n+1$ injections $a_1, a_2, \dots, a_{n+1}$ going from $S^{\otimes n}$ to $S^{\otimes(n+1)}$; a_i inserts a 1 at position i. (So the index n is suppressed.) This can be visualized as follows:

$$S \rightrightarrows S \otimes S \substack{\rightarrow\\ \rightarrow\\ \rightarrow} S \otimes S \otimes S \dots$$

If F is any functor from the category of (commutative) R-algebras to the category of abelian groups, this leads to a complex

$$F(S) \to F(S \otimes S) \to F(S \otimes S \otimes S) \to \dots,$$

where each term $F(S^{\otimes n})$ is placed in degree $n-1$, and the differential from degree $n-1$ to degree n is the alternating sum of the maps $F(a_i)$ (there are $n+1$ of them). So from degree zero to one we have $F(a_1) - F(a_2)$, and from degree one to two we have $F(a_1) - F(a_2) + F(a_3)$. The complex property (concatenation of two differentials always gives zero) is easy to check. But one can say more:

Proposition 2.1. *Let $F = \mathbb{G}_a$ be the underlying abelian group functor (so the beginning of the complex reads $S \to S \otimes S$, and the differential is $s \mapsto 1 \otimes s - s \otimes 1$). Then the complex is exact in each positive degree.*

In general, the cohomology groups of this complex are called Amitsur cohomology, written $\mathrm{H}^i_{S/R}(F)$. For instance, if $F = \mathbb{G}_a$, then $\mathrm{H}^0_{S/R}(F) = \ker(S \to S \otimes S) = R$.

It is an important fact that one can define H^0 and H^1 also for functors F with values in the category of all groups (not necessary abelian). One puts

$$\mathrm{H}^0_{S/R}(F) = \{x \in F(S) | F(a_1)(x) = F(a_2)(x)\};$$

$$\mathrm{H}^1_{S/R}(F) = \{y \in F(S \otimes S) | F(a_2)(y) = F(a_3)(y)\, F(a_1)(y)\}.$$

Note that H^1 will no longer be a group in general, only a pointed set, whose distinguished point is given by the neutral element of $F(S \otimes S)$.

In particular, if we define $\underline{\mathrm{Aut}}\, M(T) = \mathrm{Aut}_T(T \otimes_R M)$ for all R-algebras T, then by our explanations above, the first Amitsur cohomology $\mathrm{H}^1_{S/R}(\underline{\mathrm{Aut}}\, M)$ classifies the S/R-form of a given R-module M. The same holds, mutatis mutandis, if we impose extra structure.

There is no obvious structure whose $\underline{\mathrm{Aut}}$ is $\mathbb{G}_a$. But for the multiplicative group functor $\mathbb{G}_m$ there is a very natural structure having the multiplicative group $\mathbb{G}_m$ as its functor of automorphisms. For every R-algebra T, the T-automorphism group of the free rank one module T over itself is clearly $T^\times$, so $\underline{\mathrm{Aut}}\, R = \mathbb{G}_m$. On the other hand one knows the S/R-forms of R; they are exactly the projective modules of rank one trivialized by S, and modulo isomorphism they form the abelian group $\mathrm{Pic}(S/R)$. So we have:

Proposition 2.2. $\mathrm{H}^1_{S/R}(\mathbb{G}_m) = \mathrm{Pic}(S/R) = \ker(\mathrm{Pic}(R) \to \mathrm{Pic}(S))$.

If S/R is a field extension L/K, all these objects are trivial. This is true more generally. Let us look at L/K-forms of the free K-module (vectorspace) of rank n. Clearly, the automorphism functor $\underline{\mathrm{Aut}}(K^n)$ identifies with the functor $\underline{GL}_n$. From the theory of vectorspaces it is obvious that all L/K-forms of K^n are trivial, just looking at the dimension. This gives:

Proposition 2.3. *For any field extension L/K, the Amitsur cohomology $\mathrm{H}^1_{L/K}(\underline{GL}_n)$ is trivial.*

3. A few examples

(a) Let p a prime, $R = K$ a field of characteristic p, $S = L$ an extension field of K. We are considering L/K-forms in the category of Hopf algebras. Let $A = K[x, y]/(x^p, y^p)$; this becomes a K-Hopf algebra by letting x and y be primitive. We need to determine $\underline{\mathrm{Aut}}\,A$. Every automorphism of Hopf algebras respects primitive elements. Hence every Hopf automorphism of A over K restricts to an automorphism of $Kx + Ky$. One can check that a similar property also holds for all base-changed Hopf algebras ${}_TA$. Hence the functor $\underline{\mathrm{Aut}}\,A$ identifies with $\underline{GL}_2$, and therefore all L/K-forms of the Hopf algebra A are trivial.

(b) We look at the same object A again over K of characteristic p, but this time just as an algebra. Let $M = xA+yA$ be the radical of A. Then every element z of M satisfies $z^p = 0$. So for any elements $z, w \in M$ one has a well-defined algebra endomorphism sending x to z and y to w, and this will be an automorphism iff z and w are independent modulo M^2. If we now let $G_i = \{\varphi \in \mathrm{Aut}(A) | \varphi \equiv id \bmod M^i\}$, then G_0/G_1 identifies with $\underline{GL}_2$, and all higher quotients G_i/G_{i+1} are isomorphic to products of copies of $\mathbb{G}_a$. A similar discussion works, m.m., when K is replaced by any K-algebra T. There exists an appropriate version of the long exact sequence in Amitsur cohomology, attached to any short exact sequence of group-valued functors. Applying this and our previous knowledge, we again obtain that A has no nontrivial forms.

(c) Finally we put $p = 2$ and look at the same algebra $A = K[x, y]/(x^2, y^2)$, but now we take K of characteristic not 2. To be on the safe side we assume L/K Galois (separable would be enough). The picture is now quite different. In a nutshell: $x+y$ is no longer nilpotent of exponent 2. Stretching this observation a bit, one can show, for any automorphism φ of A (in principle one would have to write this down with K replaced by any finite K-algebra T without nilpotents): Modulo Kxy we either have $\varphi(x) \in K^\times x$ and $\varphi(y) \in K^\times y$, or vice versa $\varphi(x) \in K^\times y$ and $\varphi(y) \in K^\times x$. The automorphisms of the first kind form a subgroup functor $G' \subset \underline{\mathrm{Aut}}\,A$, and G' can be filtered again by subgroups such that all quotients are $\mathbb{G}_m$ or $\mathbb{G}_a$, so its first Amitsur cohomology is trivial. The entire group $\underline{\mathrm{Aut}}\,A$ is a semidirect product of G' and the two-element group C_2 that corresponds to switching x and y. And now indeed $\mathrm{H}^1_{L/K}(C_2)$ may well be non-trivial. For L/K Galois with group G, we will see that $\mathrm{H}^1_{L/K}(C_2) = \mathrm{Hom}(G, C_2)$.

One can calculate everything if L/K is a separable quadratic extension. There always exists exactly one nontrivial L/K-form of A. In the example $L/K = \mathbb{C}/\mathbb{R}$, the nontrivial form is

$$A' = \mathbb{R}[u, v]/(uv, u^2 - v^2).$$

4. Different versions of the descent mechanism

If we know more about the extension S/R than just that it is faithfully flat, then we can expect more precise and amenable results. Our goal is Galois descent; this works when S/R is Galois in the sense of Chase, Harrison and Rosenberg. Note that this implies S/R projective and faithful. In the book of Knus-Ojanguren, so-called "faithfully projective" descent is treated as an intermediary between "faithfully flat" and "Galois". We will short-circuit this, for two reasons. One of them is time. The other is that over a noetherian ring, every finitely generated flat module is already projective, so the former of the two transitions is not so dramatic. (Side remark: The typical flat modules which are not finitely generated are localizations. If one wants faithfully flat extensions, one has to take direct sums of sufficiently many localisations. This leads to another variant of descent theory: glueing objects together in the Zariski topology of $\mathrm{Spec}(R)$.)

So let us assume S/R is Galois in the mentioned sense with group G. The map $S \otimes S \to Map(G, S) = S^G$ given by $s \otimes t \mapsto (s\,\gamma(t))_{\gamma \in G}$ is then an isomorphism of S-modules.

From this one can deduce an iterated version: The map

$$S \otimes S \otimes S \to S^{G\times G}, \quad , s \otimes t \otimes u \mapsto \big(s\,\gamma(t)\,\gamma\delta(u)\big)_{\gamma,\delta \in G}$$

is likewise an isomorphism over S (which operates on $S \otimes S \otimes S$ via the leftmost factor, and on $G \times G$-tuples with entries in S in the obvious way).

Now one has two maps $d_1, d_2 : S \to S^G$ given by $d_1(s)_\gamma = \gamma(s)$, and $d_2(s)_\gamma = s$. In the same vein, there are three maps $S^G \to S^{G\times G}$ given by

$$\begin{aligned}
\partial_1(f)_{\gamma,\delta} &= \gamma(f_\delta);\\
\partial_2(f)_{\gamma,\delta} &= f_{\gamma\delta};\\
\partial_3(f)_{\gamma,\delta} &= f_\gamma
\end{aligned}$$

for each G-tuple $f \in S^G$.

The main point is now that the following diagram commutes (not too hard to check).

$$\begin{tikzcd} S \arrow[r, shift left, "a_1"] \arrow[r, shift right, "a_2"'] \arrow[d] & S \otimes S \arrow[r, shift left=2, "a_1"] \arrow[r, "a_2"] \arrow[r, shift right=2, "a_3"'] \arrow[d] & S \otimes S \otimes S \arrow[d] \\ S \arrow[r, shift left, "d_1"] \arrow[r, shift right, "d_2"'] & S^G \arrow[r, shift left=2, "\partial_1"] \arrow[r, "\partial_2"] \arrow[r, shift right=2, "\partial_3"'] & S^{G\times G}. \end{tikzcd}$$

The maps d_i and ∂_i are exactly those that show up in the definition of (non-abelian) group cohomology. Therefore we have for every group-valued functor F and every G-Galois extensions S/R of rings an identification of pointed sets

$$\mathrm{H}^1_{S/R}(F) = \mathrm{H}^1(G, F(S)).$$

If in particular $F = \underline{\mathrm{Aut}}\, A$ for an R-algebra A (say), then $\mathrm{H}^1(G, \mathrm{Aut}({}_S A))$ classifies the S/R-forms of A. The G-action on $\mathrm{Aut}({}_S A)$ is by conjugation involving the G-action on the tensor factor S. More explicitly, if A is finitely generated free over R, and an automorphism of ${}_S A$ is given as a square matrix of coefficients in S, then G simply acts on these coefficients.

Example: $\mathbb{C}/\mathbb{R}$ is Galois with $G = C_2$. Let us take $A = \mathbb{R}[t, t^{-1}]$ (the ring of functions on $\mathbb{G}_m$). Then $\mathrm{Aut}({}_\mathbb{C} A)$ is a semidirect product of $\mathbb{C}^\times$ and C_2. A nonzero scalar λ in $\mathbb{C}$ corresponds to $t \mapsto \lambda t$. The nontrivial element of C_2 corresponds to $t \mapsto 1/t$. We find

$$\mathrm{H}^1(G, \mathrm{Aut}({}_\mathbb{C} A)) = \mathrm{H}^1(G, C_2) = \mathrm{Hom}(G, C_2)$$

has two elements. The nontrivial form is well known - the ring of functions on the unit circle over $\mathbb{R}$ (Haggenmüller-Pareigis). It also carries a Hopf structure.